

**HELP, IS THERE A LAWYER IN THE HOUSE?  
HEALTHCARE PRIVACY LAWS AND TECHNOLOGY ARE CHANGING FAST!**

Thursday, September 14, 2023  
Kasowitz Benson Torres LLP, 1633 Broadway, New York, NY 10019

\*\*\*

The program content, as well as the live, non-traditional format of the program, are suitable for Experienced and Newly Admitted Attorneys.

The panel is brought to you by the Cybersecurity/Privacy/Crypto/AI Committee, and this year we will address important new developments in Healthcare Privacy. New technologies are upending how existing laws are applied, and new laws are being adopted at a rapidly intensifying pace. Whether you are a corporate advisor, regulatory specialist, or litigator, these changes could impact your clients in important ways. The program will focus on: 1) Changing Technology: How to identify and define Personal Health Information in the age of AI, online advertising and expanding privacy regulations; 2) Changing Laws: the conflict and overlap between states privacy laws, HIPAA and the FTC Act, and how to manage the increasing complexity in a privacy-compliance program; and 3) Cyber Incidents: how to protect and manage a cyber incident that compromises Personal Health Information, and the potential fallout both legally and practically from the same.

New York is the first state to require cybersecurity and data privacy CLE credits. Starting on July 1, 2023, New York now requires at least one hour of cybersecurity/data privacy CLE as a part of our 24-hour biennial CLE requirement. We are happy to announce that the September 14 panel will be the very first New York Inn of Court program to qualify.

**MATERIALS AND HANDOUTS**

1. Timed Agenda
2. HHS guidance on use of tracking technologies by HIPAA-covered entities
3. *Doe vs. Meta Platforms, Inc.*, Order on Motion to Dismiss, September 7, 2023
4. HHS HITECH Regulations
5. HHS Summary of the HIPAA Privacy Rule
6. Connecticut Public Act No. 23-56
7. Washington State "My Health My Data" Act
8. United States v. GoodRx Holding, Inc., stipulated order for permanent injunction.
9. Nevada S.B. 370
10. New York City Administrative Code section 22-1201

1

**HELP, IS THERE A LAWYER IN THE HOUSE?  
HEALTHCARE PRIVACY LAWS AND TECHNOLOGY ARE CHANGING FAST!**

Thursday, September 14, 2023  
Kasowitz Benson Torres LLP, 1633 Broadway, New York, NY 10019

\*\*\*

**Timed Agenda**

5:30-6:30: Social Hour

\*\*\*

**Speakers:** Annmarie Giblin, Susan Meekins, David Straite Eugene Kublanovsky, Manvinder Singh  
Matthew Katz, Steven Perlstein, Jason Houda, Jonny Algor and Dan Fetterman

6:30-6:35: WELCOME AND INTRODUCTION

6:35-6:55: HEALTHCARE TECHNOLOGY PANEL

6:55-7:00: Q&A

7:00-7:25: HEALTHCARE PRIVACY LAWS PANEL


7:25-7:30: Q&A

7:30-7:55: HEALTHCARE DATA BREACH PANEL

7:55-7:59: Q&A

7:59-8:00: CLOSING REMARKS AND HOUSEKEEPING FOR CLE CREDIT

2

 An official website of the United States government  
[Here's how you know](#)



## U.S. Department of Health and Human Services

Enhancing the health and well-being of all Americans

MENU

</>

Navigate to:



# Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

[Back  
to top](#)

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities<sup>1</sup> and business associates<sup>2</sup> (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”).<sup>3</sup> OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities’ noncompliance with the HIPAA Rules. A regulated entity’s failure to comply with the HIPAA Rules<sup>4</sup> may result in a civil money penalty.

Tracking technologies are used to collect and analyze information about how users interact with regulated entities’ websites or mobile applications (“apps”). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity’s health care operations.<sup>5</sup> The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI).<sup>6</sup> Some regulated entities

may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.<sup>7</sup> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures<sup>8</sup> of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.<sup>9</sup>

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule<sup>10</sup> but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [Back to top](#)

This Bulletin provides a general overview of how the HIPAA Rules apply to regulated entities' use of tracking technologies. This Bulletin addresses:

- What is a tracking technology?
- How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
  - Tracking on user-authenticated webpages<sup>11</sup>
  - Tracking on unauthenticated webpages<sup>12</sup>
  - Tracking within mobile apps<sup>13</sup>
  - HIPAA compliance obligations for regulated entities when using tracking technologies

## What is a tracking technology?

Generally, a tracking technology is a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app (“website owner” or “mobile app owner”), or third parties, to create insights about users’ online activities. Such insights could be used in beneficial ways to help improve care or the patient experience. However, this tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment.

Tracking technologies collect information and track users in various ways,<sup>14</sup> many of which are not apparent to the website or mobile app user. Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts<sup>15</sup> to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user’s mobile device-related information. For example, mobile apps may use a unique identifier from the app user’s mobile device, such as a device ID<sup>16</sup> or advertising ID.<sup>17</sup> These unique identifiers, along with any other information collected by the app, enable the mobile app owner or vendor or any other third party who receives such information to create individual profiles about each app user.<sup>18</sup>

[Back to top](#)

Website or mobile app owners may use tracking technologies developed internally or those developed by third parties. Generally, tracking technologies developed by third parties (e.g., tracking technology vendors) send information directly to the third parties who developed such technologies and may continue to track users and gather information about them even after they navigate away from the original website to other websites. This Bulletin focuses on regulated entities’ obligations when using third party tracking technologies.

### **How do the HIPAA Rules apply to regulated entities’ use of tracking technologies?**

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity’s website or mobile app, including individually identifiable health information (IIHI)<sup>19</sup> that the individual provides when they use regulated entities’ websites or mobile apps. This information might include an individual’s medical record number, home or email address, or dates of

appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.<sup>20</sup> All such IHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.<sup>21</sup> This is because, when a regulated entity collects the individual's IHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.<sup>22</sup>

### ***Tracking on user-authenticated webpages***

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI. Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI)<sup>23</sup> collected through its website is protected and secured in accordance with the HIPAA Security Rule.<sup>24</sup>

Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.*, health care operations<sup>25</sup>) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules.<sup>26, 27</sup> For example, if an individual makes an appointment through the website of a



covered health clinic<sup>28</sup> for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.

### ***Tracking on unauthenticated webpages***

Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, services they provide, or their policies and procedures. Tracking technologies on regulated entities' unauthenticated webpages generally do not have access to individuals' PHI; in this case, a regulated entity's use of such tracking technologies is not regulated by the HIPAA Rules. **However**, in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include:

- The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal, generally are unauthenticated because the individual did not provide credentials to be able to navigate to those webpages. However, if the individual enters credential information on that login webpage or enters registration information (e.g., name, email address) on that registration page, such information is PHI.<sup>29</sup> Therefore, if tracking technologies on a regulated entity's patient portal login page or registration page collect an individual's login information or registration information, that information is PHI and is protected by the HIPAA Rules.
- Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

## ***Tracking within mobile apps***

Mobile apps<sup>30</sup> that regulated entities offer to individuals (e.g., to help manage their health information, pay bills) collect a variety of information provided by the app user, including information typed or uploaded into the app, as well as information provided by the app user's device, such as fingerprints,<sup>31</sup> network location, geolocation, device ID, or advertising ID. Such information collected by a regulated entity's mobile app is PHI, and thus the regulated entity must comply with the HIPAA Rules for any PHI that the mobile app uses or discloses, including any subsequent disclosures to the mobile app vendor, tracking technology vendor, or any other third party who receives such information. For example, the HIPAA Rules apply to any PHI collected by a covered health clinic through the clinic's mobile app used by patients to track health-related variables associated with pregnancy (e.g., menstrual cycle, body temperature, contraceptive prescription information).

However, the HIPAA Rules do not protect the privacy and security of information that users voluntarily download or enter into mobile apps that are not developed or offered by or on behalf of regulated entities, regardless of where the information came from. For example, the HIPAA Rules do not apply to health information that an individual enters into a mobile app offered by an entity that is not regulated by HIPAA (even if the individual obtained that information from their medical record created by a regulated entity). In instances where the HIPAA Rules do not apply to such information, other law may apply. For instance, the Federal Trade Commission (FTC) Act and the FTC's Health Breach Notification Rule (HBNR) may apply in instances where a mobile health app impermissibly discloses a user's health information.<sup>32</sup>

## **HIPAA compliance obligations for regulated entities when using tracking technologies**

Regulated entities are required to comply with the HIPAA Rules when using tracking technologies. Some examples of the HIPAA Privacy, Security, and Breach Notification requirements that regulated entities must meet when using tracking technologies with access to PHI include:

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.<sup>33</sup>
  - Regulated entities may identify the use of tracking technologies in their website or mobile app’s privacy policy, notice, or terms and conditions of use.<sup>34</sup> However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.<sup>35</sup>
  - If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals’ HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website’s use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.
  - Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals’ authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

Back  
to top

- Establishing a BAA with a tracking technology vendor that meets the definition of a “business associate.”
  - A regulated entity should evaluate its relationship with a tracking technology vendor to determine whether such vendor meets the definition of a business associate and ensure that the disclosures made to such vendor are permitted by the Privacy Rule. A tracking technology vendor is a business associate if it meets the definition of a business associate, regardless of whether the required BAA is in place.<sup>36</sup> Moreover, signing an agreement containing the elements of a BAA does not make a tracking technology vendor a business associate if the tracking technology vendor does not meet the business associate definition.
  - The BAA must specify the vendor’s permitted and required uses and disclosures of PHI and provide that the vendor will safeguard the PHI and report any security incidents, including breaches of unsecured PHI, to the regulated entity, among other requirements.<sup>37</sup>
  - If a regulated entity does not want to create a business associate relationship with these vendors, or the chosen tracking technology vendor will not provide written satisfactory assurances in the form of a BAA that it will appropriately safeguard PHI, then the entity cannot disclose PHI to the vendors without individuals’ [Back to top](#) authorizations.
- Addressing the use of tracking technologies in the regulated entity’s Risk Analysis and Risk Management processes,<sup>38</sup> as well as implementing other administrative, physical, and technical safeguards in accordance with the Security Rule (e.g., encrypting ePHI that is transmitted to the tracking technology vendor;<sup>39</sup> enabling and using appropriate authentication, access, encryption, and audit controls when accessing ePHI maintained in the tracking technology vendor's infrastructure)<sup>40</sup> to protect the ePHI.
- Providing breach notification<sup>41</sup> to affected individuals, the Secretary, and the media (when applicable) of an impermissible disclosure of PHI to a tracking technology vendor that compromises the security or privacy of PHI when there is no Privacy Rule requirement or permission to disclose PHI and there is no BAA with the vendor. In such instances, there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised.<sup>42</sup>

## Filing a Privacy Complaint

If you believe that your (or someone else's) health privacy rights have been violated, visit the OCR complaint portal at <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf> <<https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>> to file a complaint online.

**DISCLAIMER:** The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or the Departments' policies.

To obtain this information in an alternate format, contact the HHS Office for Civil Rights at (800) 368-1019, TDD toll-free: (800) 537-7697, or by emailing [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov). Language assistance services for OCR matters are available and provided free of charge.

## Resources

HIPAA Guidance:

- Health Apps: <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html> <<https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html>>
- Security Rule: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es> Back to top
- Cybersecurity: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html> <<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>>
- Privacy Rule: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html> <<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html>>
- Business Associate Contracts: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html> <<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>>

For more information on health apps and online tracking, visit:

- FTC Guidance on online tracking: <https://consumer.ftc.gov/articles/how-protect-your-privacy-online> <<https://consumer.ftc.gov/articles/how-protect-your-privacy-online>>

- FTC Guidance for mobile health apps:
  - <https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool> <<https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool>>
  - <https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act> <<https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act>>
  - <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use> <<https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use>>
- FTC Health Breach Notification Rule: <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule> <<https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>>
- ONC’s Model Privacy Notice for technology developers: <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf> - PDF <<https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>>

Back  
to top

---

## Endnotes:

<sup>1</sup> See 45 CFR 160.103 (definition of “Covered entity”).

<sup>2</sup> See 45 CFR 160.103 (definition of “Business associate”).

<sup>3</sup> See 45 CFR parts 160 and 164. See *also* OCR’s Fact Sheet on Direct Liability of Business Associates, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html> <<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>>

<sup>4</sup> See 42 USC 1320d-5; see *also* 45 CFR part 160, subpart D; and 2019 Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, 84 FR 18151 (April 30, 2019). For more information on breach reporting, see also OCR’s Guidance on the Breach Notification Rule, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> <<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>>.

<sup>5</sup> Health care operations include customer service, business planning and development, and business management or general administrative activities. See 45 CFR 164.501 (definition of “Health care operations”). This Bulletin does not address all potential purposes for which a regulated entity might use tracking technologies and the specific conditions that apply to uses and disclosures for those purposes. For example, uses and disclosures of PHI for purposes of research, such as research studies that involve the collection of PHI using tracking technologies, are not within the scope of this bulletin; those uses and disclosures are subject to the requirements of the Privacy Rule’s research provisions at 45 CFR 164.512(i).

<sup>6</sup> See 45 CFR 160.103 (definition of “Protected health information”).

<sup>7</sup> See, e.g., <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> <<https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>> [↗](#) </disclaimer.html> and <https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2796236> <<https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2796236>> [↗](#) </disclaimer.html>.

<sup>8</sup> Regulated entities can use or disclose PHI, without an individual’s written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. See 45 CFR 164.502(a).

<sup>9</sup> See 45 CFR 164.508(a)(3); see *also* 45 CFR 164.501 (definition of “Marketing”).

<sup>10</sup> 45 CFR part 160 and subparts A and E of part 164.

<sup>11</sup> This Bulletin uses the term “user-authenticated webpages” to refer to webpages that users can access only **after** they log in to the webpage, such as by entering a unique user ID and password or other credentials.

<sup>12</sup> This Bulletin uses the term “unauthenticated webpages” to refer to webpages that are publicly accessible without first requiring a user to log in to such webpage.

<sup>13</sup> A mobile app is a software program for mobile devices. This Bulletin uses the term “mobile apps” to refer to apps offered to individuals by regulated entities to allow the individuals to, for example, find providers, access or manage their health information or health care, or pay bills.

Back  
to top

<sup>14</sup> See FTC Report on Cross-Device Tracking, <https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017> <<https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017>>.

<sup>15</sup> Cookies are files placed on a user's device to customize a user's browsing experience but can also be used to track a user's activities. A web beacon or tracking pixel is a tiny graphic image (usually 1 pixel) placed on a webpage that allows the website owner or a third party to collect information regarding the use of the webpage that contains the web beacon. Session replay scripts record a user's activities (e.g., mouse movements, clicks, and typing) when using a webpage or app. Fingerprinting uses a browser's and/or device's unique configurations and settings to track user activity.

<sup>16</sup> A device ID is a unique string of numbers and letters associated with a smartphone or similar mobile device.

<sup>17</sup> An advertising ID is a unique string of numbers and letters assigned to smartphones or similar mobile devices that allows advertisers to track user activity.

<sup>18</sup> For additional information on the collection of sensitive information obtained from tracking technologies, see <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> <<https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>>. Back  
to top

<sup>19</sup> Generally, individually identifiable health information is a subset of health information, including demographic information collected from an individual, that is received by a covered entity (or its business associate) or employer; relates to the past, present, or future health, health care, or payment for health care to an individual; and identifies the individual or can be used to identify the individual. See 45 CFR 160.103 (definition of "Individually identifiable health information").

<sup>20</sup> For more information on identifiers under the Privacy Rule, see 45 CFR 164.514(b).

<sup>21</sup> There are limited situations in which an IP address or geographic location by itself may not be PHI, such as where the individual uses a computer at a public library instead of using their personal electronic device. This is because the IP address or geographic location will not be related to the individual when using a public device. However, even in



such cases, the IP address or geographic location from such devices, combined with any information provided by users through a webpage or mobile app, could be used to identify the individual and therefore may be PHI.

<sup>22</sup> See “Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule”, 78 FR 5566, 5598 (January 25, 2013).

<sup>23</sup> See 45 CFR 160.103 (definition of “Electronic protected health information”).

<sup>24</sup> See 45 CFR part 164, subparts A and C.

<sup>25</sup> See 45 CFR 164.506; see *also* 45 CFR 164.501 (definition of “Health care operations”).

<sup>26</sup> See 45 CFR 164.504(e) and 45 CFR 164.308(b).

<sup>27</sup> See OCR’s Fact Sheet on Direct Liability of Business Associates, *supra* note 3.

<sup>28</sup> A health clinic is covered if it is a health care provider that transmits any health information in electronic form in connection with a transaction covered by 45 CFR 162. Back  
to top

<sup>29</sup> See 45 CFR 160.103 (definition of “Electronic media”); see *also* 45 CFR 160.103 (defining “Protected health information” as “individually identifiable health information . . . that is transmitted by electronic media; maintained by electronic media; or transmitted or maintained in any other form or medium”).

<sup>30</sup> For additional resources for mobile health app developers, see <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html> <<https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html>>.

<sup>31</sup> A mobile device fingerprint typically includes information such as the device name, type, operating system version, and IP address.

<sup>32</sup> For more information on the privacy and security of personal consumer apps, see <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html> <<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html>>.

<sup>33</sup> See 45 CFR 164.502(a), 45 CFR 164.502(b), and 45 CFR 164.514(d).

<sup>34</sup> See, e.g., <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf> - PDF <<https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>>.

<sup>35</sup> See 45 CFR 164.502(a) and 164.502(e).

<sup>36</sup> See, e.g., 45 CFR 164.308(b)(3) and 45 CFR 164.502(e)(2).

<sup>37</sup> See, e.g., 45 CFR 164.504(e); and 45 CFR 164.314(a). See also OCR's Sample Business Associate Contract, <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html> <<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>>.

<sup>38</sup> See 45 CFR 164.308.

<sup>39</sup> A regulated entity must implement encryption for ePHI in transit and at rest if it is a reasonable and appropriate safeguard. If it is not reasonable and appropriate, the regulated entity must document why not and implement an equivalent alternative measure if reasonable and appropriate. See 45 CFR 164.312(a)(2)(iv); 45 CFR 164.312(a)(ii); and 45 CFR 164.306(d). See also OCR's HIPAA FAQ #2020, <https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html> <<https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html>>.

<sup>40</sup> See 45 CFR 164.308(a)(4); 45 CFR 164.312(a); 45 CFR 164.312(b); and 45 CFR 164.312(d).

<sup>41</sup> See 45 CFR 164.402 (definition of "Breach").

<sup>42</sup> See 45 CFR 164.400 *et seq.* Impermissible disclosures of health information by non-HIPAA regulated entities may be subject to the FTC's Health Breach Notification Rule. See 16 CFR 318 *et seq.*

---

Content created by Office for Civil Rights (OCR)






Content last reviewed December 1, 2022

## Sign Up for Email Updates

Receive the latest updates from the Secretary, Blogs, and News Releases.

**Sign Up** <<https://cloud.connect.hhs.gov/subscriptioncenter>>

<<https://hhs.gov>>

				
< <a href="https://www.facebook.com/hhs">https://www.facebook.com/hhs</a> >	< <a href="https://twitter.com/witte/hhs">https://twitter.com/witte/hhs</a> >	< <a href="https://www.youtube.com/channel/UC...">https://www.youtube.com/channel/UC...</a> >	< <a href="https://www.instagram.com/hhs">https://www.instagram.com/hhs</a> >	< <a href="https://www.linkedin.com/company/hhs">https://www.linkedin.com/company/hhs</a> >

^  
Back  
to top

### HHS Headquarters

200 Independence Avenue, S.W.  
Washington, D.C. 20201  
Toll Free Call Center: 1-877-696-6775

3

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, et al.,  
Plaintiffs,  
v.  
META PLATFORMS, INC., et al.,  
Defendants.

Case No. [22-cv-03580-WHO](#)

**ORDER ON MOTION TO DISMISS**

Plaintiffs challenge defendant Meta Platform, Inc.’s alleged use of proprietary computer code to obtain certain healthcare-related information of Facebook users: according to plaintiffs, the Meta Pixel allows Meta to intercept personally identifiable medical information and the content of patient communications from Facebook users, which Meta then monetizes for its own financial gain. Plaintiffs have brought several federal and state law claims, some of which they have plausibly alleged and others which need more specificity. As explained below, Meta’s motion is GRANTED in part and DENIED in part.

**BACKGROUND**

Plaintiffs are five Facebook users who are proceeding anonymously due to the sensitive nature of this litigation. Consolidated Class Action Complaint (“CCAC,” Dkt. 185) ¶¶ 24-28. They allege that Meta improperly acquires their confidential health information in violation of state and federal law and in contravention of Meta’s own policies regarding use and collection of Facebook users’ data. *Id.* ¶¶ 1–2, 5, 7.

Each of plaintiffs’ healthcare providers—MedStar Health System, Rush University System for Health, WakeMed Health & Hospitals, Ohio State University Wexner Medical Center, and North Kansas City Hospital—allegedly installed the Meta Pixel on its patient portals. *See id.* ¶¶ 24-28. Plaintiffs claim that when they logged into their patient portal on their medical provider’s

1 website, the Pixel transmitted information to Meta. *Id.* ¶¶ 6, 8-13, 22. They contend that this  
2 information, contemporaneously redirected to Meta, revealed their status as patients and was  
3 monetized by Meta for use in targeted advertising. *Id.* ¶¶ 9, 13.

4 Plaintiffs initially moved for a preliminary injunction. Dkt. No. 46. I denied that motion,  
5 finding that while plaintiffs presented sufficient evidence of a “weighty injury,” the scope of their  
6 injury and technical feasibility of plaintiffs’ proposed solutions were not clear and the balance of  
7 equities and public interest factors did not support injunctive relief based on the record at that  
8 juncture. Dkt. No. 159 (“PI Order”).

9 In February 2023, Interim Class Counsel filed their Consolidated Class Action Complaint.  
10 Dkt. No. 185. In the CCAC, plaintiffs expand the scope of their suit and bring 13 claims: (1)  
11 breach of contract; (2) breach of the duty of good faith and fair dealing; (3) violation of the  
12 Electronic Communications Privacy Act (“ECPA” or “Wiretap Act”); (4) violation of the  
13 California Invasion of Privacy Act (“CIPA”); (5) intrusion upon seclusion; (6) California  
14 constitutional invasion of privacy; (7) negligence per se; (8) trespass to chattels; (9) violation of  
15 California’s Unfair Competition Law (“UCL”); (10) violation of California’s Consumer Legal  
16 Remedies Act (“CAFA”); (11) larceny; (12) violation of California’s Comprehensive Computer  
17 Data Access and Fraud Act (“CDAFA”); and (13) unjust enrichment.

18 Defendant has moved to dismiss each of the claims asserted in the CCAC.<sup>1</sup>

### 19 LEGAL STANDARD

20 Under FRCP 12(b)(6), a district court must dismiss a complaint if it fails to state a claim  
21 upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must  
22 allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v.*  
23 *Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts  
24 that “allow the court to draw the reasonable inference that the defendant is liable for the  
25 misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). There must  
26 be “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* While courts do not  
27

28 <sup>1</sup> In moving for a preliminary injunction, plaintiffs relied on their claims under the ECPA, CIPA,  
and California tort law. Dkt. No. 46.

1 require “heightened fact pleading of specifics,” a plaintiff must allege facts sufficient to “raise a  
2 right to relief above the speculative level.” *Twombly*, 550 U.S. at 555, 570.

3 In deciding whether the plaintiff has stated a claim upon which relief can be granted, the  
4 Court accepts the plaintiff’s allegations as true and draws all reasonable inferences in favor of the  
5 plaintiff. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However,  
6 the court is not required to accept as true “allegations that are merely conclusory, unwarranted  
7 deductions of fact, or unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049,  
8 1055 (9th Cir. 2008). If the court dismisses the complaint, it “should grant leave to amend even if  
9 no request to amend the pleading was made, unless it determines that the pleading could not  
10 possibly be cured by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir.  
11 2000). In making this determination, the court should consider factors such as “the presence or  
12 absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by  
13 previous amendments, undue prejudice to the opposing party and futility of the proposed  
14 amendment.” *Moore v. Kayport Package Express*, 885 F.2d 531, 538 (9th Cir. 1989).

## 15 DISCUSSION

### 16 I. ELECTRONIC COMMUNICATIONS PRIVACY ACT – CLAIM 3

17 “The Wiretap Act prohibits the unauthorized ‘interception’ of an ‘electronic  
18 communication.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606–07 (9th Cir.  
19 2020), cert. denied sub nom. *Facebook, Inc. v. Davis*, 141 S. Ct. 1684 (2021) (quoting 18 U.S.C. §  
20 2511(1)(a)–(e)). To state this claim, plaintiffs must plausibly allege that Meta (1) intentionally (2)  
21 intercepted (3) the contents of (4) plaintiffs’ electronic communications (5) using a device. *See In*  
22 *re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (listing ECPA elements).

#### 23 A. Intent

24 Addressing the intent and intercept elements of the ECPA claim in the PI Order, I wrote:

25 “Intercept” is defined under the Wiretap Act as “the aural or other  
26 acquisition of the contents of any wire, electronic, or oral  
27 communication through the use of any electronic, mechanical, or  
28 other device.” 18 U.S.C. § 2510(4). Although the statute does not  
define “acquisition,” the Ninth Circuit has construed the term  
according to its ordinary meaning as the “act of acquiring, or coming  
into possession of [.]” *United States v. Smith*, 155 F.3d 1051, 1055

1 n.7 (9th Cir. 1998). “Such acquisition occurs when the contents of a  
2 wire communication are captured or redirected in any way.” *Noel v.*  
3 *Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (internal citation and  
4 quotation marks omitted).

5 According to plaintiffs, the Pixel is “designed for the very purpose  
6 of intercepting communications on third-party websites by  
7 surreptitiously and contemporaneously redirecting these  
8 communications to Meta.” Mot. at 11 (citing Smith Decl. ¶¶ 7–14).  
9 Plaintiffs have put forward evidence that Meta receives information  
10 through the Pixel. *See, e.g.*, Smith Decl. ¶¶ 4–5, 32–33. Meta does  
11 not dispute that the intentional or interception elements are met. *See*  
12 *Opp.* at 20–21. Plaintiffs appear likely to succeed on these two  
13 elements of their claim.

14 PI Order at 18.

15 Meta points out that it did not dispute the intent element at the preliminary injunction  
16 stage. It disputes it now, arguing that plaintiffs have failed to plausibly allege that Meta  
17 intentionally – meaning “purposefully and deliberately and not as a result of accident or mistake,”  
18 *United States v. Christensen*, 828 F.3d 763, 790 (9th Cir. 2015) – intended to intercept their  
19 sensitive health information. It asserts that plaintiffs cannot meet this burden because the CCAC  
20 acknowledges that third-party web developers, not Meta, choose whether to install Pixel and also  
21 set parameters on what information to send to Meta. It also argues that intent cannot be alleged  
22 because, as plaintiffs acknowledge, Meta seeks to avoid receiving sensitive information by  
23 contractually forbidding developers from sending it and filtering out any potentially sensitive data  
24 it detects on the back end. Mot at 5-6 (citing CCAC ¶¶ 39, 44-46 (Pixel is customizable per  
25 instructions provided by Meta), 118, 125, 148-149 (Meta has systems in place to filter sensitive  
26 information and, has publicly stated it does not want sensitive health information)).

27 While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it  
28 intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta  
29 *really* intends. *See, e.g.*, CCAC ¶¶ 122-123, 144-146, 150, 161 (plaintiffs allege Meta’s tools and  
30 filters are not effective, not fully implemented, and call into question Meta’s true intent). What  
31 Meta’s true intent is, what steps it actually took to prevent receipt of health information, the  
32 efficacy of its filtering tools, and the technological feasibility of implementing other measures to  
33 prevent the transfer of health information, all turn on disputed questions of fact that need  
34 development on a full evidentiary record. *See, e.g., Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684



1 (N.D. Cal. 2021) (“At the pleading stage, however, interception may be considered intentional  
2 ‘where a defendant is aware of the defect causing the interception but takes no remedial action.’”)  
3 (quoting *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020)). At this  
4 stage, intent has been adequately alleged.

### 5 **B. Content**

6 Meta also argues that plaintiffs have not and cannot plausibly plead interception of covered  
7 “content.” The statute broadly defines “content” to include “any information concerning the  
8 substance, purport, or meaning of [a] communication.” 18 U.S.C. § 2510(8). “Contents” refers to  
9 the “intended message conveyed by the communication”—it does not include record information  
10 regarding the characteristics of the message that is generated in the course of the communication.  
11 *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). For instance, contact  
12 information provided as part of a sign-up process constitutes “content” because this information is  
13 the subject of the communication. *Id.* at 1107 (“Because the users had communicated with the  
14 website by entering their personal medical information into a form provided by the website, the  
15 First Circuit correctly concluded that the defendant was disclosing the contents of a  
16 communication.”). And while a URL that includes “basic identification and address information”  
17 is not “content,” a URL disclosing a “search term or similar communication made by the user”  
18 “could constitute a communication” under the statute. *Id.* at 1108–09.

19 In the PI Order, I found that plaintiffs had made a strong showing on this element:

20 In my view, the log-in buttons and the kinds of descriptive URLs  
21 identified in the Smith Decl. are “contents” within the meaning of the  
22 statute. Unlike in *Zynga*, the URLs at issue here would not merely  
23 reveal the name of a Facebook user or group—as Smith explained,  
24 the transmitted URLs include both the “path” and the “query string.”  
25 Smith Decl. ¶¶ 50–51; see also *id.* ¶ 189 (showing  
26 [hardfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis](http://hardfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis) URL).

25 These items are content because they concern the substance of a  
26 communication. *See Zynga*, 750 F.3d at 1107; *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) (“If an address, phone number, or URL is . . . part of the substantive information conveyed to the recipient, then by definition it is ‘content.’”); see also *In re Google RTB Consumer Priv. Litig.*, No. 21-cv-2155-YGR, 2022 WL 2165489, at \*10 (N.D. Cal. June 13, 2022) (finding that categories of the website, categories that describe the current section of the website, and referrer URL that caused

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

navigation to the current page constituted “content”).

PI Order at 19. Meta acknowledges this prior conclusion, but argues that unspecified “remaining items” that are transferred “mostly” do not qualify as content and claims based on “those communications” should be dismissed. Mot. at 9-10; Reply at 4.

At this juncture, plaintiffs have adequately alleged covered content is transferred. The boundaries of what transferred information is content under the Act is better determined on a full evidentiary record.

**C. Consent**

Finally, Meta argues that the ECPA’s one-party consent exemption (exempting liability for intercepted information resulting from one party’s consent) bars the claim as a matter of law. Meta points out, again, that it is the third-party web developers who make their Pixel-enhanced websites available to plaintiffs and their other healthcare customers, and by doing so those healthcare entities have necessarily consented to the transmission of data to Meta.

In the PI Order, I explained:

[T]he Wiretap Act exempts liability in certain circumstances. The statute provides that:

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d). In other words, the Wiretap Act allows interception where the interception is made by a “party” to the communication or where a “party” has consented to the interception. *Id.* This exception does not apply, however, where the interceptor acts “for the purpose of” committing any crime or tort in violation of state or federal law. *Id.*

PI Order at 20.<sup>2</sup>

---

<sup>2</sup> In the PI Order, I “put aside” the issue of consent and considered whether the “crime or tort” “exception to the exception” applied. I concluded there was a “not-insignificant chance, then, that plaintiffs may be able to show that the crime-tort exception applies,” but “in light of the authority in this district finding that liability does not lie where a defendant’s primary motivator was to make money, I am not convinced that plaintiffs have met their burden to show that the law and facts ‘clearly favor’ their position.” *Id.* at 20-22. However, I noted “this claim will present

1 On this motion to dismiss, the issue of consent is front and center and the burden of proof  
2 to show this exemption applies is on Meta. See *In re Google RTB Consumer Priv. Litig.*, 606 F.  
3 Supp. 3d 935, 949 (N.D. Cal. 2022). In support of dismissal, Meta relies on *Katz-Lacabe v.*  
4 *Oracle Am., Inc.*, No. 22-CV-04792-RS, 2023 WL 2838118, at \*10 (N.D. Cal. Apr. 6, 2023).  
5 There, plaintiffs challenged Oracle’s collection of “personal information from internet users” by  
6 “synchroniz[ing] that data to create individual profiles, and ultimately sell[ing] that data—  
7 bolstered by data made available by its partners—on its Data Marketplace.” The court dismissed  
8 the ECPA claim because, “[a]s Defendant’s customers must have chosen to deploy Oracle’s tools  
9 on their websites, it necessarily follows that ‘one of the parties to the communication’—the  
10 websites themselves—gave ‘prior consent to such interception.’” *Id.* at \*210 (relying on  
11 *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at \*6 (N.D. Cal. May 21,  
12 2021).

13 Plaintiffs counter with *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL  
14 5029899, at \*9 (N.D. Cal. Aug. 7, 2023). There, the court rejected summary judgment on the  
15 consent issue under the ECPA claim, despite the defendant having “generally disclosed” its data  
16 tracking practices, because it also “promote[d] the privacy afforded by Incognito” as a browsing  
17 mode. *Id.* In that situation, Google “itself created a situation where there is a dispute as to whether  
18 users’ consent of Google’s data collection generally is ‘substantially the same’ as their consent to  
19 the collection of their private browsing data in particular.” *Id.*

20 The facts alleged here – that while Meta disclosed its purported attempts to prevent third-  
21 party developers who incorporated the Pixel from sending sensitive data to Meta, Meta in fact  
22 intended to receive and did receive that sensitive data – bring this case closer to *Brown. Id.*, 2023  
23 WL 5029899 \*7 (“For consent to be actual, the disclosures must ‘explicitly notify’ users of the  
24 practice at issue.”). Meta has not pointed to anything I can judicially notice on this motion to  
25 dismiss to show as a matter of law that the healthcare providers did not just presumably but  
26

27 \_\_\_\_\_  
28 differently in a motion to dismiss context,” and recognized that the “parties will have the  
opportunity to refine their arguments regarding Meta’s purpose in intercepting the information at  
issue here later in the litigation.” PI Order at 20-22.

1 *actually* consented to the sending of sensitive healthcare information of its customers.

2 Determination of whether actual consent was given depends on what Meta disclosed to healthcare  
3 providers, how it described and trained healthcare providers on the Pixel, and how the healthcare  
4 providers understood the Pixel worked and the information that then could or would be collected  
5 by Meta. These evidence-bound determinations are inappropriate to reach on this motion.

6 Meta’s motion to dismiss the ECPA claim is DENIED.

7 **II. CALIFORNIA INVASION OF PRIVACY ACT – CLAIM 4**

8 In the PI Order, I concluded that plaintiffs had adequately alleged and supported their  
9 CIPA claim under both sections 631(a) and 632, based on Meta’s challenges to “content” under  
10 631(a) and “confidential communications” under 632. PI Order at 23-24. Meta now moves to  
11 dismiss the California state law analog to the ECPA, raising arguments not addressed in my PI  
12 Order.

13 **A. Extraterritoriality**

14 Meta initially argues that CIPA does not apply “extraterritorially,” because CIPA’s intent  
15 is “to protect the right of privacy of the people of this state.” Cal. Penal Code § 630. As none of  
16 the named plaintiffs are California residents, Meta contends the CIPA claim must be dismissed.

17 I disagree for three reasons. First, this contention is arguably premature. *Kellman v.*  
18 *Spokeo, Inc.*, 599 F. Supp. 3d 877, 894 (N.D. Cal. 2022), *motion to certify appeal denied*, No.  
19 3:21-CV-08976-WHO, 2022 WL 2965399 (N.D. Cal. July 8, 2022) (deferring choice of law  
20 analyses until class certification, after discovery shed light on whether defendants’ acts had a  
21 substantial nexus to California).

22 Second, plaintiffs have plausibly alleged that the conduct at issue, in terms of the design  
23 and marketing of the Pixel technology and development and implementation of its Terms of  
24 Service, occurred in California;. *See, e.g., Schmitt v. SN Servicing Corp.*, No. 21-CV-03355-  
25 WHO, 2021 WL 3493754, at \*3 (N.D. Cal. Aug. 9, 2021) (data breach allegations regarding  
26 defendant who operated out of California “sufficient to allow out-of-state plaintiffs to seek  
27 recovery under California law”); *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1028 (N.D.  
28 Cal. 2011) (“A legislative purpose that articulates an interest in protecting those within California

1 is not inconsistent with also allowing non-Californians to pursue claims against California  
 2 residents.”); *see also Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018), *certified*  
 3 *question accepted sub nom. Oman v. Delta Air Lines*, No. S248726, 2018 WL 10809386 (Cal. July  
 4 11, 2018), *and certified question answered*, 9 Cal. 5th 762 (2020) (“If the conduct that ‘creates  
 5 liability’ occurs in California, California law properly governs that conduct.”).

6 Third, Facebook’s Terms of Service specify that California law applies to disputes between  
 7 Facebook and its users. CCAC ¶ 292. That alone may not be dispositive, but it supports allowing  
 8 these non-resident plaintiffs to assert a claim against a California resident under CIPA. *See*  
 9 *Maldonado v. Apple, Inc.*, No. 3:16-CV-04067-WHO, 2021 WL 1947512, at \*6 (N.D. Cal. May  
 10 14, 2021) (“California Supreme Court held that choice-of-law clauses in contracts are generally  
 11 enforceable and laid out a multipart test to determine whether to follow the contracted-for  
 12 jurisdiction’s law or disregard it.”).

13 I am not determining or foreclosing any choice-of-law issues. Choice-of-law has not been  
 14 squarely raised. I am denying the motion to dismiss the CIPA claim based on Meta’s  
 15 extritoriality argument.

16 **B. Intent**

17 Meta also argues plaintiffs fail to allege plausible facts to support the intent element of  
 18 CIPA, which requires a showing of Meta’s “affirmative desire” to intercept communications.  
 19 Intent under CIPA is determined consistently with intent under ECPA, and for the same reasons as  
 20 discussed above, intent has been adequately alleged. Whether Meta’s affirmative disclosures and  
 21 back-end filtering process sufficiently negate intent depends on Meta’s knowledge as well as its  
 22 implementation and the efficacy of its alleged contractual efforts and back-end filtering. Those  
 23 will be tested on an evidentiary record. Similarly, Meta’s point that Pixel captures some data that  
 24 healthcare entities may permissibly share with Meta might provide a defense to some portion of  
 25 plaintiffs’ CIPA claim, but it does not negate the plausible allegations that sensitive healthcare  
 26 information is intentionally captured and transmitted to Meta.

27 **C. Sent or Received**

28 Meta points out that CIPA only covers interception of a communication while “it is being

1 sent from, or received at any place within this state,” Cal. Penal Code § 631(a), and argues  
 2 plaintiffs have not plausibly alleged that plaintiffs’ information was being sent to or received from  
 3 a place in this state. Plaintiffs plead that Meta is headquartered in California and Meta “designed  
 4 and *effectuated* its scheme to track the patient communications at issue here from California.”  
 5 CCAC ¶ 369 (emphasis added). That is sufficient at this stage.

#### 6 **D. Device**

7 The last CIPA challenge is whether the Pixel is a “device” under Section 632(a) because it  
 8 is a piece of software. Meta points out that two judges in this District, when considering  
 9 “electronic tracking devices” under Penal Code section 637.7(d), have rejected the argument that  
 10 tracking software are “devices.” *See In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 193  
 11 (N.D. Cal. 2019) (Davila, E.) (Google maps software and related “services are not a ‘device’  
 12 within the meaning of Section 637.7(d).”); *In Moreno v. San Francisco Bay Area Rapid Transit*  
 13 *Dist.*, 2017 WL 6387764, at \*5 (N.D. Cal. Dec. 14, 2017) (Corley, J.) (an “electronic tracking  
 14 device” does not include “software installed in mobile devices”).

15 Plaintiffs respond that the section 637.7 cases so not apply to this section 632(a) case.  
 16 They instead discuss decisions construing and interpreting CIPA consistently with the ECPA  
 17 which hold that servers or software qualify as “devices” under the ECPA. *Oppo*. at 10 n.2.<sup>3</sup> Most  
 18 on point is *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015). There, plaintiffs  
 19 alleged that a software application, once installed on users’ phones, “surreptitiously intercepted  
 20 personal data and communications and transmitted this data to Carrier IQ and its customers.” *Id.*  
 21 The Honorable Edward M. Chen held that “plaintiffs have sufficiently alleged that the Carrier IQ  
 22 Software is a ‘device’ for purposes of the Wiretap Act.” *Id.* at 1084. The section 637.7 cases are  
 23

---

24 <sup>3</sup> A few of the cases plaintiffs rely on are not truly in support. For example, in *United States v.*  
 25 *Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010), as amended (Nov. 29, 2010), the court held  
 26 that the defendant “acquired the emails by using at least three devices: Infusino’s computer (where  
 27 the rule was set up), the Kansas City server (where the rule caused each message to be duplicated  
 28 and sent his way), and his own computer (where the messages were received, read, and sometimes  
 stored).” In *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 690 (N.D. Cal. 2021), the court simply  
 found that “Apple used the devices [iPhone] by programming Siri software to intercept  
 communications when no hot word was spoken”). In both cases, devices were used. Here the use  
 allegations concern only software.

1 distinguishable, and absent contrary authority under section 632(a), I agree that the Pixel software  
2 is a device under section 632(a).

3 Meta’s motion to dismiss the CIPA claim is DENIED.

4 **III. CONSTITUTIONAL PRIVACY (CLAIM 6) AND INTRUSION ON SECLUSION**  
5 **(CLAIM 5)**

6 Addressing the invasion of privacy and intrusion on seclusion claim in the PI Order, I  
7 explained that plaintiffs had shown enough to demonstrate a reasonable expectation of privacy in  
8 their medical communications (despite Meta’s policies generally disclosing its collection of data  
9 from users and its disclosures that it would require partners to obtain lawful rights to share  
10 protected user data) and that Meta’s conduct was highly offensive. PI Order at 24-27. Meta  
11 argues here that the California’s constitutional privacy protections do not apply extraterritorially  
12 and plaintiffs have failed to adequately allege their sensitive information was received by Meta.

13 As with CIPA, plaintiffs have plausibly alleged that the conduct causing them harm  
14 occurred in and emanated from California. That is sufficient at this juncture.

15 Concerning the protected interest, Meta argues that plaintiffs have failed to plausibly allege  
16 a violation of their constitutionally protected privacy interests because the named plaintiffs fail to  
17 identify with specificity what, if any, private or particularly sensitive information about them Meta  
18 allegedly received. Meta is correct that these named plaintiffs do not identify in the CCAC what  
19 specific, personal or private information they conveyed to their healthcare providers that they  
20 reasonably believe Meta received.

21 In opposition, plaintiffs do not dispute this or identify any particular categories of  
22 information that they shared with their healthcare providers that they reasonably believe was  
23 captured by Meta. Instead, they rely on *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d  
24 589 (9th Cir. 2020) to argue they do not need to disclose the specific information they contend  
25 Meta received. But in that case, there was no dispute that Facebook collected “a full-string  
26 detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and  
27 the name of the precise file requested,” when it operated. *Id.* at 605. Here, as Meta repeatedly  
28 points out and plaintiffs admit, there is information collected by the Pixel software that does not

1 constitute sensitive, personal information.

2           Given the nature of this case – where plaintiffs allege that both unprotected and  
3 constitutionally protected information was captured by Meta’s Pixel – plaintiffs are required to  
4 amend to describe the types or categories of sensitive health information that they provided  
5 through their devices to their healthcare providers. That basic amendment (which can be general  
6 enough to protect plaintiffs’ specific privacy interests) will allow these privacy claims to go  
7 forward.<sup>4</sup>

8           Plaintiffs’ invasion of privacy claims are DISMISSED with leave to amend.

9 **IV. CALIFORNIA’S COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD**  
10 **ACT – CLAIM 12**

11           CDAFA provides that only an individual who has “suffer[ed] damage or loss by reason of  
12 a violation” of the statute may bring a civil action “for compensatory damages and injunctive  
13 relief or other equitable relief.” Cal. Penal Code § 502(e)(1). CDAFA permits recovery of  
14 “[c]ompensatory damages [that] include any expenditure reasonably and necessarily incurred by  
15 the owner or lessee to verify that a computer system, computer network, computer program, or  
16 data was or was not altered, damaged, or deleted by the access.” *Id.*

17 **A. Loss or Damage**

18           Meta initially seeks dismissal of plaintiffs’ CDAFA claim because plaintiffs have not  
19 alleged and cannot allege “damage or loss” in an action like this that is based on privacy violations  
20 as opposed to an intrusion that impacts the performance or operation of computer devices. Meta  
21 relies on a recent decision from Chief Magistrate Judge Donna M. Ryu, *Cottle v. Plaid Inc.*, 536 F.  
22 Supp. 3d 461 (N.D. Cal. 2021), where Judge Ryu rejected a theory of loss or damage under  
23 CDAFA based on the “loss of the right to control their own data, the loss of the value of their data,

---

24 <sup>4</sup> Related to the “legally protected interest” argument, Meta also contends that the privacy claims  
25 fail because plaintiffs have not alleged a “sufficiently serious” invasion of their privacy rights.  
26 Once plaintiffs amend to identify the types of protected information they shared with their  
27 healthcare providers and was likely captured by Meta, they will have plausibly alleged a  
28 sufficiently serious impact on their privacy rights. *See* PI Order at 26-27. Meta’s remaining  
arguments, that its filtering efforts and purported use of any received healthcare information are  
highly relevant to whether its conduct is “highly offensive,” have merit. Mot. at 14-15. But the  
balancing of the various factors required by *Hill v. Nat’l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 37  
(1994), must be done on a full evidentiary record.



1 and the loss of the right to protection of the data,” as that type of loss was not covered by the  
 2 statute. *Id.* at 488 (citing *Nowak v. Xapo, Inc.*, No. 5:20-cv-03643-BLF, 2020 WL 6822888, at \*4-  
 3 5 (N.D. Cal. Nov. 20, 2020) (dismissing CDAFA claim based on loss of value of stolen  
 4 cryptocurrency in part because the nature of the loss was not cognizable under CDAFA)).

5 Plaintiffs respond that they adequately allege actionable “loss or damage” under CDAFA  
 6 by alleging: (1) the Pixel “has precluded” them from being able to communicate with their  
 7 healthcare providers through their computers or otherwise and (2) their protected information is  
 8 diminished in value. Plaintiffs cite a number of cases from this District that they claim support  
 9 these types of damages under CDAFA. However, each of the cases plaintiffs rely on dealt with  
 10 different sections of CDAFA or allegations of impaired device performance. *Oppo.* at 13.<sup>5</sup>

11 Plaintiffs provide no support for their argument that an “inability” to use their computer  
 12 devices to communicate with their healthcare providers in the future is a cognizable form of loss  
 13 or damage actionable under the CDAFA. Their diminished value of information claim is  
 14 foreclosed by the reasoning in *Cottle*.

15 Plaintiffs indicated at the hearing that they might be able to plead a different theory of  
 16 impairment of their computing devices. They may do so. The CDAFA claim is DISMISSED,  
 17 with leave to amend.

### 18 **B. Other CDAFA Elements**

19 Meta also attacks the substance of the CDAFA claim. The CCAC relies on various  
 20 substantive sections of CDAFA: sections 502(c)(1), (c)(2), (c)(3), (c)(6), (c)(7), and (c)(8). In  
 21 opposition plaintiffs address only (1) and (8).<sup>6</sup> In their further amended CCAC, plaintiffs shall  
 22

---

23 <sup>5</sup> See *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 454 (N.D. Cal. 2018), on  
 24 reconsideration in part, 386 F. Supp. 3d 1155 (N.D. Cal. 2019) (addressing (c)(4) and (c)(5) and  
 25 allegations of device impairment); *Ubisoft, Inc. v. Kruk*, No. CV 20-478-DMG (ASX), 2021 WL  
 26 3472833, at \*4 (C.D. Cal. July 9, 2021) ((c)(5) claim alleging DDoS attacks); *In re Carrier IQ,*  
 27 *Inc.*, 78 F. Supp. 3d 1051, 1067 (N.D. Cal. 2015) (alleging impact on battery life and  
 28 performance); see also *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir.  
 2020) (finding Article III standing to allege CDAFA claim, but not addressing standing under the  
 “loss or damage” requirement of the statute).

<sup>6</sup> These provisions hold persons liable for “(1) Knowingly accesses and without permission alters,  
 damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer  
 network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or

United States District Court  
Northern District of California

1 limit the CDAFA claim to these two subsections only.

2 Meta argues that plaintiffs have not alleged a claim under (1) because intent has not been  
3 sufficiently alleged. Consistent with the ECPA and CIPA discussions above, however, plaintiffs  
4 have adequately alleged intent. Meta next contends that plaintiffs cannot plausibly allege a claim  
5 under (8), as it was the healthcare entities’ web developers who introduced Pixel onto their own  
6 websites, not Meta. Plaintiffs’ allegations regarding how Meta induced or encouraged those  
7 entities to adopt and install the Pixel suffice at this juncture.

8 Meta also asserts that even if it could be vicariously liable, plaintiffs have not alleged and  
9 cannot plausibly allege that the Pixel is a prohibited “contaminant.”<sup>7</sup> In *In re iPhone Application*  
10 *Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) the court explained:

11 Section 502(c)(1[2]) defines “computer contaminant” as “any set of  
12 computer instructions that are designed to modify, damage, destroy,  
13 record, or transmit information within a computer, computer system,  
14 or computer network without the intent or permission of the owner of  
15 the information. They include, but are not limited to, a group of  
16 computer instructions commonly called viruses or worms. . . to  
17 contaminate other computer programs or computer data, consume  
18 computer resources, modify, destroy, record, or transmit data, or in  
19 some other fashion usurp the normal operation of the computer,  
20 computer system, or computer network.” *See* Cal.Penal Code § 502(b)  
(10) (emphasis added). Thus, the very definition of a “computer  
21 contaminant” limits liability to conduct that occurs “without the intent  
22 or permission of the owner of the information.” Moreover, the section  
23 on “computer contaminants” appears to be aimed at “viruses or  
24 worms,” and other malware that usurps the normal operation of the  
25 computer or computer system. Although Plaintiffs[] are given leave  
26 to amend to clarify their allegations in an amended complaint, it is not  
27 clear to the Court how Section 502(c)(8) applies to the case at hand.”

28 *Id.* at \*13.

extort, or (B) wrongfully control or obtain money, property, or data” and (8) “Knowingly  
introduces any computer contaminant into any computer, computer system, or computer network.”  
Cal. Penal Code § 502(c).

<sup>7</sup> Cal. Penal Code § 502(12) “‘Computer contaminant’ means any set of computer instructions  
that are designed to modify, damage, destroy, record, or transmit information within a computer,  
computer system, or computer network without the intent or permission of the owner of the  
information. They include, but are not limited to, a group of computer instructions commonly  
called viruses or worms, that are self-replicating or self-propagating and are designed to  
contaminate other computer programs or computer data, consume computer resources, modify,  
destroy, record, or transmit data, or in some other fashion usurp the normal operation of the  
computer, computer system, or computer network.”

1 Whether plaintiffs can, on amendment, plausibly allege facts establishing recognized “loss  
2 or damage” sufficient to state a claim under CDAFA will also inform whether the Pixel is a  
3 contaminant that “usurps” the normal operation of plaintiffs’ devices. *See also Flextronics Int’l,*  
4 *Ltd. v. Parametric Tech. Corp.*, No. 5:13-CV-00034-PSG, 2014 WL 2213910, at \*5 (N.D. Cal.  
5 May 28, 2014) (“a plaintiff need only allege that the actions of the contaminant  
6 (modify/damage/destroy/record/ transmit) were undertaken by overcoming a technical barrier  
7 without the permission of the owner; the introduction of the contaminant to the system need not  
8 surmount the same hurdle.”).

9 The motion to dismiss the CDAFA claim is GRANTED with leave to amend.

10 **V. BREACH OF CONTRACT – CLAIMS 1 & 2**

11 **A. Limitation of Liability in Meta’s Terms of Service**

12 Meta argues initially that a “limitation of liability” clause in its TOS bars the breach of  
13 contract claims. That clause provides: “[Meta]’s liability shall be limited to the fullest extent  
14 permitted by applicable law, and under no circumstance will we be liable to you for any lost  
15 profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or  
16 incidental damages arising out of or related to these Terms or the Meta Products.” Meta RJN Ex.  
17 1 at 7.<sup>8</sup>

18 Meta notes that at least one court in this District has applied Meta’s limitation provision to  
19 defeat express and implied contract claims, rejecting the argument that the limitation provision  
20 was unconscionable. *See Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037 (N.D. Cal. 2019)  
21 (“Perhaps regrettably, ‘[w]ith respect to claims for breach of contract, limitation of liability  
22 clauses are enforceable unless they are unconscionable, that is, the improper result of unequal  
23 bargaining power or contrary to public policy.’ *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*,  
24 209 Cal. App. 4th 1118, 1126, 147 Cal.Rptr.3d 634 (2012).”). The *Bass* court then determined  
25 that the limitations provision was not unconscionable as applied to the contract and quasi-contract  
26

27 <sup>8</sup> Meta seeks judicial notice of various documents, including its TOS, Business Tools Terms,  
28 Commercial Terms, Privacy Policy and Cookies Policy. *See* Dkt. No. 232-1. Plaintiffs do not  
oppose the request. The request is GRANTED.

1 causes of action. *Id.* at 1038; *see also Darnaa, LLC v. Google LLC*, 756 F. App'x 674, 676–77  
2 (9th Cir. 2018) (rejecting unconscionability argument, “[a]s interpreted by California courts,  
3 Section 1668 generally does not prohibit parties from limiting liability for breach of contract,  
4 including breach of the implied covenant. [citations omitted]. We see no reason to depart from this  
5 principle here.”).

6 Plaintiffs respond that Meta’s attempt to limit its liability for the breach claim runs afoul of  
7 California Civil Code section 1668. It provides: “All contracts which have for their object,  
8 directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to  
9 the person or property of another, or violation of law, whether willful or negligent, are against the  
10 policy of the law.” Here, because defendants acted intentionally by refusing to stop the data  
11 transfer or employ a stronger filter mechanism, plaintiffs assert that section 1668 comes into play  
12 even for a breach of contract claim. On that basis, they distinguish *Bass* from this case as *Bass*  
13 concerned a negligent data breach case caused by an obscure flaw in Meta’s code and Meta took  
14 immediate action to fix it.

15 In addition to the substantive differences between the allegations in *Bass* and this case,  
16 plaintiffs also note that other courts in this district have allowed breach of contract claims to  
17 continue against Facebook despite the limitation of liability clause. *See, e.g., Lundy v. Facebook*  
18 *Inc.*, No. 18-CV-06793-JD, 2021 WL 4503071, at \*2 (N.D. Cal. Sept. 30, 2021) (“For the  
19 damages element of plaintiffs’ contract and quasi-contract claims, plaintiffs have adequately  
20 pleaded claims for disgorgement and nominal damages. [] These types of damages are not  
21 covered by the limitation of liability provision Facebook points to in its motion to dismiss. []  
22 Nominal damages may be recovered for a breach of contract under California law.” (internal  
23 citations omitted)); *Shared.com v. Meta Platforms, Inc.*, No. 22-CV-02366-RS, 2022 WL  
24 4372349, at \*4 (N.D. Cal. Sept. 21, 2022) (allowing breach of contract and other claims to  
25 proceed past motion to dismiss stage despite limitation of liability clause because the “discovery  
26 process would aid in determining more concretely whether each claim avers direct or indirect  
27 damages. The limitations provision will therefore not mandate dismissal of any of Plaintiff’s  
28 claims, though Defendant can always reassert the limitations provision in, for example, a motion

1 for summary judgment”).

2 Here, plaintiffs have pleaded entitlement to nominal damages and restitution. CCAC ¶  
3 317. Given the differences between the damages sought as well as the intentional conduct alleged  
4 (distinguishing this case from *Bass*), the breach of contract claims will not be dismissed based on  
5 the limitation of liability clause. Meta may, however, move to limit the types of damages  
6 available (*e.g.*, anything beyond nominal damages) on summary judgment or at another  
7 appropriate juncture.

8 **B. Sufficiently Definite Promises and Breach**

9 Next Meta argues that the contractual provisions on which plaintiffs based their breach of  
10 contract claim are not “sufficiently definite.” The specific contractual promises made in Meta’s  
11 Privacy Policy and TOS and plaintiffs’ allegations regarding breach are identified at paragraph  
12 312 in the CCAC:

- 13 • “We require Partners to have the right to ... share your information before giving it to us.”

14 Plaintiffs allege: “Meta does not require Partners to have the right to share health  
15 information with Meta before giving it to Meta.”

- 16 • “We employ dedicated teams around the world ... to detect potential misuse of our  
17 Products, harmful conduct towards others, and situations where we may be able to help  
18 support or protect our community.”

19 Plaintiffs allege: “Meta does not employ dedicated teams to prevent its  
20 unauthorized acquisition of health information. To the contrary, Meta employs  
21 dedicated teams to encourage health entities to share health information with Meta  
22 that the health entities lack rights to share.”

- 23 • “We ... develop advanced technical systems to detect potential misuse of our Products,  
24 harmful conduct towards others, and situations where we may be able to help support or  
25 protect our community. If we learn of content or conduct like this, we will take appropriate  
26 action – for example ... removing content, blocking access to certain features, disabling an  
27 account, or contacting law enforcement.”

28 Plaintiffs allege: “Meta has developed advanced technical systems to detect  
potential misuse of certain products and is fully capable of using those systems to  
detect Pixel Partners from which it is acquiring health information without  
authorization. However, Meta has not used those systems to stop acquiring such  
information and has not taken appropriate action to prevent health entities from  
sharing health information with Meta in the absence of the right to do so.”

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- “We work with external service providers, partners, and other relevant entities ... to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content.”

Plaintiffs allege: “Meta does not work with external service providers, Partners, or other relevant entities to detect potential misuse of sending health information to Meta through the Pixel without the right to do so. To the contrary, Meta works with Partners to help those Partners avoid the meaningless restrictions Meta places on ads that are targeted to health. As shown above, Meta teaches health entities how to avoid its “restrictions” on personalized health targeted ads by removing certain words that would give users the idea that the ad was specifically targeted to them, all the while continuing to target ads to specific users based on personal attributes, including health.”

CCAC ¶ 312; *see also* ¶¶ 96-97 (noting Meta “requires” some information including sensitive and protected information from users for services to work), 117 (same).<sup>9</sup> Plaintiffs’ specific references to identified provisions in Meta’s TOS and Privacy Policy are sufficiently definite to “determine the scope of the duty and the limits of performance must be sufficiently defined to provide a rational basis for the assessment of damages.” *Ladas v. California State Auto. Assn.*, 19 Cal. App. 4th 761, 770 (1993).

Plaintiffs have also plausibly alleged that Meta breached the promises. Meta overreads the impact of plaintiffs’ “admissions” that Meta may have “discouraged” partners from sending sensitive or protected information and Meta employed a filter to reduce the transfer of sensitive or protected information. Meta ignores plaintiffs’ detailed and plausible allegations regarding how and why the transfer of sensitive or protected information is necessary for Meta’s advertising services to function in the way Meta advertised those services, as well as allegations that Meta knew its filter was not effective and could have improved its filter or taken other steps to block the transfer of the sensitive or protected information. That is sufficient at this juncture.

The motion to dismiss the breach of contract and related breach of the duty of good faith and fair dealing claims is DENIED.<sup>10</sup>

---

<sup>99</sup> In addressing consent at the preliminary injunction stage, as both sides here note, I expressed that Meta’s use of the term “require” was susceptible to multiple meanings. PI Order at 16.

<sup>10</sup> Plaintiffs’ covenant of good faith and fair dealing claim is based on allegations that Meta abused its power in interpreting “require” in a way that does not actually require anything. CCAC ¶ 323;

**VI. UNJUST ENRICHMENT – CLAIM 13**

Meta moves to dismiss the unjust enrichment claim, which California law construes as a quasi-contract claim, in light of plaintiffs’ express contract claim. But plaintiffs may plead this claim as an alternative at this juncture, even if the contract claim can be read to cover plaintiffs’ allegation that Meta sold their data without consent and unjustly retained the proceeds. *See Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015). Meta also argues that the claim cannot stand as plaintiffs have failed to plead that they lack adequate remedies at law under *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). But plaintiffs do allege that their remedies at law are inadequate. *See* CCAC ¶¶ 448, 489.

The motion to dismiss the unjust enrichment claim is DENIED.

**VII. NEGLIGENCE PER SE – CLAIM 7**

Under California law, negligence per se is not a separate cause of action, but a negligence claim analyzed under the per se doctrine. *See Dent v. Nat'l Football League*, 902 F.3d 1109, 1118 (9th Cir. 2018). Under that doctrine, the standard of care can be established by a statute, and a defendant’s violation of that statute can “give rise to a presumption that it failed to exercise due care” where that violation “proximately caused an injury,” the injury resulted from something the statute was designed to prevent, and the person who was injured was “one of the class of persons for whose protection the statute, ordinance, or regulation was adopted.” *Id.* (internal citations omitted). However, the basic elements of a negligence claim, including duty of care and causation, must still be alleged. *See Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256, 1285 (2006).

Meta attacks plaintiffs’ attempt to plead a breach of the duty of care required to state a negligence-based claim. Plaintiffs’ only identified source of duty is HIPAA, and at least one court this District and another within the Ninth Circuit have rejected HIPAA as a basis of a negligence per se claim. *See, e.g., Austin v. Atlina*, No. 20-CV-6363-YGR, 2021 WL 6200679, at \*3 (N.D.

---

Oppo. at 17. As construed, the claim is not merely duplicative of or exceeding the obligations imposed by the contractual provisions plaintiffs rely on for their express breach claim. Plaintiffs have also adequately Meta’s intent – conscious and deliberative acts – given the breach allegations discussed above. *See Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (Cal. Ct. App. 1990).

1 Cal. Dec. 22, 2021) (“Because there is no private right of action under HIPAA, plaintiff’s HIPAA  
 2 claim is not cognizable under common law”); *Teeter v. Easterseals-Goodwill N. Rocky Mountain,*  
 3 *Inc.*, No. CV-22-96-GF-BMM, 2023 WL 2330241, at \*4 (D. Mont. Mar. 2, 2023) (dismissing  
 4 negligence per se cause of action based on HIPAA); *see also Delta Sav. Bank v. United States*, 265  
 5 F.3d 1017, 1026 (9th Cir. 2001) (“[t]o bring suit under the FTCA based on negligence per se, a  
 6 duty must be identified, and this duty cannot spring from a federal law. The duty must arise from  
 7 state statutory or decisional law, and must impose on the defendants a duty to refrain from  
 8 committing the sort of wrong alleged here,” and citing authority explaining “[t]he pertinent inquiry  
 9 is whether the duties set forth in the federal law are analogous to those imposed under local tort  
 10 law”) (quotations omitted); *In re: Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL  
 11 1810606, at \*16 (D. Minn. June 2, 2022) (“Here, Plaintiffs have not cited any precedent in  
 12 California, Minnesota, Nevada, South Carolina, or Wisconsin that permits a state-law negligence  
 13 per se claim to proceed based on the theory that there is a violation of Section 5 of the FTC Act.”);  
 14 *but see In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1143 (C.D. Cal. 2021)  
 15 (allowing negligence/negligence per se claim based on violations of FTCA and HIPAA to  
 16 proceed).<sup>11</sup>

17 Following the majority of the cases that have considered the issue, the negligence per se  
 18 claim based on a duty created by HIPAA is DISMISSED with leave to amend so that plaintiffs  
 19 may attempt to identify a state law source of the duty of care.

## 20 **VIII. TRESPASS TO CHATTELS – CLAIM 8**

21 Under California law, trespass to chattels “lies where an intentional interference with the  
 22 possession of personal property has proximately caused injury.” *Intel Corp. v. Hamidi*, 30 Cal.4th  
 23 1342, 1350–51, 1 Cal.Rptr.3d 32, 71 P.3d 296 (2003). This claim does not lie where injuries are  
 24 to privacy and confidentiality. *See Casillas v. Berkshire Hathaway Homestate Ins. Co.*, 79 Cal.

25  
 26  
 27 <sup>11</sup> Meta also challenges plaintiffs’ ability to plausibly please causation for a negligence claim,  
 28 given plaintiffs’ admission that the healthcare providers’ web developers, not Meta, choose what  
 information the Pixel sends to Meta. Mot. at 21. Given plaintiffs’ plausible allegations that Meta  
 induced or encourages web developers to send protected or sensitive private information,  
 causation is sufficiently alleged at this juncture.



1 App. 5th 755, 765 (2022). In cases of interference with possession of personal property not  
2 amounting to conversion “the owner has a cause of action for trespass or case, *and may recover*  
3 *only the actual damages suffered by reason of the impairment of the property or the loss of its*  
4 *use.” Hamidi*, at 1351 (emphasis in original, quoting *Zaslow v. Kroenert*, 29 Cal. 2d 541, 551  
5 (1946)); *see also id.* 1353 (where there was “no actual or threatened damage to [plaintiff’s]  
6 computer hardware or software and no interference with its ordinary and intended operation,” the  
7 defendant’s trespass was not actionable); *In re iPhone Application Litig.*, No. 11-MD-02250-LHK,  
8 2011 WL 4403963, at \*13–14 (N.D. Cal. Sept. 20, 2011 (following *Hamidi* and dismissing a  
9 privacy-based action where plaintiffs failed to connect the trespass to a harm in the functioning of  
10 the phone).

11 Plaintiffs’ trespass claim is based on their assertions that Meta places the \_fbp cookie on  
12 their devices via their health-care providers’ websites. They do not allege that the presence of that  
13 cookie “impairs” the operation of their devices in terms of diminished storage, decreased battery  
14 life, or otherwise. Instead, they assert that Meta’s tracking diminishes the value of plaintiffs’  
15 computing devices because plaintiffs no longer want to use their devices to communicate with  
16 their healthcare providers. CCAC ¶¶ 415-28, 423-25. They analogize their inability to use their  
17 phones and computers to communicate with their healthcare providers (lest they disclose personal  
18 healthcare information) to the situation in *Grace v. Apple Inc.*, No. 17-CV-00551, 2017 WL  
19 3232464, at \*11 (N.D. Cal. July 28, 2017). There, based on allegations that Apple heavily  
20 advertised the presence and ability to use Facetime in its iPhones and allegations that use of  
21 Facetime was integral to the plaintiffs’ use of their iPhones, the court allowed the trespass claim to  
22 continue because the removal of Facetime from plaintiffs’ phones due to Apple’s software update  
23 significantly impaired the value of plaintiffs’ phones.

24 Here, unlike in *Grace*, there are no allegations that any functionality inherent in their  
25 computing devices has been impacted by Meta’s conduct. Nor are there allegations that plaintiffs  
26 purchased any specific computing device with the purpose in whole or part of using that device to  
27 communicate with their healthcare providers. That these plaintiffs may have valued using their  
28 personal devices to communicate with their healthcare providers does not sufficiently impair the

1 value of those devices to allow the plaintiffs to state a trespass to chattels claim.

2 The trespass claim is DISMISSED with leave to amend.

3 **IX. LARCENY – CLAIM 11**

4 Plaintiffs’ larceny claim is brought under California Penal Code sections 484 and 496(a),<sup>12</sup>  
 5 based on the theory that Meta “knowingly obtained” plaintiffs’ information “by false pretenses.”  
 6 CCAC ¶¶ 455-464; Oppo. at 20-21; *see also Bell v. Feibush*, 212 Cal. App. 4th 1041, 1047-48  
 7 (2013) (discussing theft by false pretenses). To plausibly state a theft by false pretenses claim,  
 8 plaintiffs must allege not only that Meta made specific false representations to them, but also that  
 9 plaintiffs transferred their property to Meta “in reliance on the representation.” *See People v.*  
 10 *Miller*, 81 Cal. App. 4th 1427, 1440 (2000), as modified on denial of reh’g (July 6, 2000).  
 11 Plaintiffs have not clearly identified the specific representations that Meta made to them that  
 12 support their larceny claim or the facts showing that their reliance on those representations  
 13 is insufficient to state this claim.

14 The larceny claim is DISMISSED with leave to amend.

15 **X. UNFAIR COMPETITION LAW (CLAIM 9) AND CONSUMERS LEGAL  
 16 RREMEDIES ACT (CLAIM 10)**

17 A UCL claim may only be brought by “a person who has suffered injury in fact and has  
 18 lost money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204.  
 19 Plaintiffs, therefore, must “demonstrate some form of economic injury,” such as surrendering  
 20 more or acquiring less in a transaction, having a present or future property interest diminished,  
 21 being deprived of money or property, or entering into a transaction costing money or property that  
 22 would otherwise have been unnecessary. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323  
 23 (2011).

24 Courts in this district have dismissed cases where, like here, the injury is based on “the loss  
 25 of the inherent value of their personal data,” *see Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 484  
 26 (N.D. Cal. 2021), as well as where it was undisputed that plaintiffs paid no money to the

27 \_\_\_\_\_  
 28 <sup>12</sup> California Penal Code section 484 forbids theft, which includes obtaining property “by ... false  
 ... representation or pretense.” Cal. Penal Code § 484. California Penal Code section 496(a)  
 prohibits the obtaining of property “in any manner constituting theft.” Cal. Penal Code § 496(a).

1 defendant. *See In re Facebook, Inc., Consumer Privacy*, 402 F. Supp. 3d at 804 (noting “the  
2 plaintiffs here do not allege that they paid any premiums (or any money at all) to Facebook to  
3 potentially give rise to standing under California law” for purposes of UCL claim and dismissing  
4 claim for failure to allege “lost money or property”); *Wesch v. Yodlee, Inc.*, No. 20-cv-05991-SK,  
5 2021 WL 1399291, at \*6 (N.D. Cal. Feb. 16, 2021) (holding that the plaintiffs had not alleged that  
6 they “surrender[ed] more or acquir[ed] less in a transaction than they otherwise would have” for  
7 purposes of UCL standing where they had not paid money to the defendant).

8 Plaintiffs rely on *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613  
9 F. Supp. 3d 1284, 1301 (S.D. Cal. 2020). But the injury in that case was based on a “benefit-of-  
10 the-bargain” theory that plaintiffs “acquired less” in their transactions with the defendant (who  
11 sold medical devices to plaintiffs). *See also Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015,  
12 1019 (N.D. Cal. 2019) (benefit-of-the-bargain theory asserted by customers of defendant). There  
13 is no benefit of the bargain basis alleged in the CCAC with respect to the UCL claim, although  
14 benefit of the bargain allegations are made in support of the contract claim. *See* CCAC ¶ 316  
15 (seeking benefit of the bargain contract damages). Given the different requirements to state a  
16 plausible remedy under a breach of contract claim and “loss of money or property” under the  
17 UCL, a cognizable “benefit of the bargain” theory has not adequately been alleged as a remedy for  
18 the UCL claim.<sup>13</sup>

19 With respect to diminished value of their data, in the most recent Northern District case to  
20 address the issue the Hon. Richard S. Seeborg reviewed recent cases and held:

21 Plaintiffs fail to show they have an economic injury. Plaintiffs do  
22 identify some support for the idea that personal information without  
23 consent constitutes economic injury. *See Calhoun v. Google LLC*, 526  
24 F. Supp. 3d 605, 636 (N.D. Cal. 2021) (“[T]he Ninth Circuit and a  
25 number of district courts, including this Court, have concluded that  
26 plaintiffs who suffered a loss of their personal information suffered  
economic injury and had standing.”) (citing cases, including *In re  
Facebook Privacy Litig.* (“*Facebook Privacy*”), 572 F. App'x 494,  
494 (9th Cir. 2014); and *In re Yahoo! Inc. Cust. Data Sec. Breach*

27 <sup>13</sup> Plaintiffs also rely on *Callahan v. PeopleConnect, Inc.*, No. 20-CV-09203-EMC, 2021 WL  
28 5050079, at \*19 (N.D. Cal. Nov. 1, 2021), motion to certify appeal denied, No. 20-CV-09203-  
EMC, 2022 WL 2132912 (N.D. Cal. June 14, 2022), but that case dealt with the misuse of names  
and likenesses as intellectual property.

1           *Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at \*13 (N.D. Cal.  
2           Aug. 30, 2017)). The weight of the authority in the district and the  
3           state, however, point in the opposite direction: that “the ‘mere  
4           misappropriation of personal information’ does not establish  
5           compensable damages.” *Pruchnicki v. Envision Healthcare Corp.*,  
6           845 F. App'x 613, 615 (9th Cir. 2021) [citations omitted]. Because  
7           Plaintiffs have not alleged a specific monetary or economic loss,  
8           Plaintiffs lack standing to maintain their UCL claims.

9           *Katz-Lacabe v. Oracle Am., Inc.*, No. 22-CV-04792-RS, 2023 WL 2838118, at \*8 (N.D. Cal. Apr.  
10           6, 2023).

11           Judge Seeborg relied in part on *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515,  
12           538 (2022), *review denied* (Dec. 14, 2022). There, the California Court of Appeal held that  
13           plaintiffs’ “lost-value-of-PII theory, as pled, is insufficient to support UCL standing,” because  
14           “[a]ppellants properly pled only that their PII was stolen and disseminated, and that a market for it  
15           existed. They did not allege they ever attempted or intended to participate in this market, or  
16           otherwise to derive economic value from their PII. Nor did they allege that any prospective  
17           purchaser of their PII might learn that their PII had been stolen in this data breach and, as a result,  
18           refuse to enter into a transaction with them, or insist on less favorable terms. In the absence of any  
19           such allegation, appellants failed to adequately plead that they lost money or property in the form  
20           of the value of their PII.” *Id.* at 538.

21           Plaintiffs rely on *Brown v. Google LLC*, No. 20-CV-03664-LHK, 2021 WL 6064009 (N.D.  
22           Cal. Dec. 22, 2021). There, the Honorable Lucy H. Koh found that plaintiffs adequately alleged  
23           lost money or property sufficient to state their UCL claim where they alleged that “because  
24           Google previously has paid individuals for browsing histories, it is plausible that, had Plaintiffs  
25           been aware of Google’s data collection, they would have demanded payment for their data. Thus,  
26           by inducing Plaintiffs to give Google their data without payment, Google caused Plaintiffs to  
27           ‘acquire in a transaction less[ ] than [they] otherwise would have.’ [ ] Second, because there are  
28           several browsers and platforms willing to pay individuals for data, it is plausible that Plaintiffs  
29           will decide to sell their data at some point. Indeed, each named Plaintiff has alleged that he or she  
30           is aware of these browsers and platforms. [ ] Accordingly, by obtaining Plaintiffs’ data and selling  
31           it to advertisers, Google ‘diminished’ Plaintiffs’ ‘future property interest.’ *Kwikset*, 51 Cal. 4th at  
32           324.” *Brown*, at \*15.

1 Here, plaintiffs contend their allegations bring them closer to *Brown* and satisfy the  
2 deficiencies identified in *Moore*. See CCAC ¶¶ 22 (alleging Meta “takes patients’ property and  
3 property rights without compensation and ignores their right to control the dissemination of their  
4 health information to third parties”), 215 (“Meta itself has paid users for their digital  
5 information”). But the crux of *this* case concerns Meta’s receipt of “individually identifiable  
6 health information,” that plaintiffs apparently do not want Meta or anyone other than their  
7 healthcare providers to have. *Id.*, ¶¶ 1, 216 (“Americans typically do not want to see their  
8 individually identifiable health information for any purpose”). That brings it closer to *Moore* and  
9 *Katz-Lacabe*.

10 In light of the failure to separately allege a benefit of the bargain basis for “loss of money  
11 or property” under the UCL and in light of the inconsistent allegations regarding how plaintiffs  
12 could *and* would participate in a legitimate market for health care information, the UCL claim is  
13 DISMISSED with leave to amend.

14 There is a different deficiency with plaintiffs’ claim under the CLRA. The CLRA claim is  
15 based on Meta’s representation “that it required its Partners to have the right to collect, use and  
16 share Plaintiffs’ and Class members’ information but doing nothing to ensure their rights were  
17 protected.” CCAC ¶¶ 451-453. As a result, plaintiffs allege that Meta violated section 1770(2) of  
18 the CLRA by “[m]isrepresenting the source, sponsorship, approval, or certification of goods or  
19 services”; section 1770(5) of the CLRA by “[r]epresenting that goods or services have  
20 sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not  
21 have”; and section 1770(14) of the CLRA by “[r]epresenting that a transaction confers or involves  
22 rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.”

23 Meta moves to dismiss these misrepresentations claims under Rule 9(b) because none of  
24 the plaintiffs allege that they saw and relied on those alleged misrepresentations. See, e.g., *In re*  
25 *Zoom Video Commc'ns Inc. Priv. Litig.*, 525 F. Supp. 3d 1017, 1046 (N.D. Cal. 2021) (dismissing  
26 CLRA claims where “[n]o Plaintiff alleges reading those allegedly misleading statements, let  
27 alone reading them at a specific time or place.”). Plaintiffs did not address this issue in their  
28 opposition or during the hearing. In accordance with my tentative ruling, the CLRA claim is

United States District Court  
Northern District of California

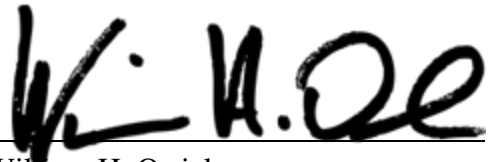
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISMISSED with leave to amend so that plaintiffs can plead facts regarding reliance on the alleged misrepresentations.<sup>14</sup>

**CONCLUSION**

For the foregoing reasons Meta’s motion is DENIED regarding the ECPA, CIPA, breach of contract, and unjust enrichment claims. The motion is GRANTED with leave to amend on the privacy, CDAFA, negligence per se, trespass, larceny, UCL, and CLRA claims. Plaintiffs shall file their amended complaint within twenty (20) days of the date of this Order.

Dated: September 7, 2023



William H. Orrick  
United States District Judge

---

<sup>14</sup> In my Tentative Order issued in advance of the hearing, I indicated I was inclined to follow Judge Koh’s decision in *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021). Dkt. No. 298. However, the defendant in *Calhoun* moved to dismiss arguing only that there was no property interest in browsing data and that copying data did not amount theft. *Id.* Meta’s argument here rests on plaintiffs’ failure to satisfy the false statement and reliance elements of that claim.

4

---

**U.S. Department of Health and Human Services  
Office for Civil Rights**



**HIPAA Administrative Simplification**

***Regulation Text***

**45 CFR Parts 160, 162, and 164  
(Unofficial Version, as amended through March 26, 2013)**

---



# HIPAA Administrative Simplification

## Table of Contents

<u>Section</u>	<u>Page</u>
<b>PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS.....</b>	<b>10</b>
<b>SUBPART A—GENERAL PROVISIONS .....</b>	<b>10</b>
§ 160.101 Statutory basis and purpose.....	10
§ 160.102 Applicability.....	11
§ 160.103 Definitions.....	11
§ 160.104 Modifications.....	17
§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.....	17
<b>SUBPART B—PREEMPTION OF STATE LAW .....</b>	<b>17</b>
§ 160.201 Statutory basis.....	17
§ 160.202 Definitions.....	18
§ 160.203 General rule and exceptions.....	18
§ 160.204 Process for requesting exception determinations.....	19
§ 160.205 Duration of effectiveness of exception determinations. ....	19
<b>SUBPART C—COMPLIANCE AND INVESTIGATIONS.....</b>	<b>19</b>
§ 160.300 Applicability.....	19
§ 160.302 [Reserved].....	20
§ 160.304 Principles for achieving compliance.....	20
§ 160.306 Complaints to the Secretary.....	20
§ 160.308 Compliance reviews.....	20
§ 160.310 Responsibilities of covered entities and business associates.....	20

§ 160.312	Secretarial action regarding complaints and compliance reviews.....	21
§ 160.314	Investigational subpoenas and inquiries.....	21
§ 160.316	Refraining from intimidation or retaliation.....	23
<b>SUBPART D—IMPOSITION OF CIVIL MONEY PENALTIES .....</b>		<b>23</b>
§ 160.400	Applicability.....	23
§ 160.401	Definitions.....	23
§ 160.402	Basis for a civil money penalty.....	23
§ 160.404	Amount of a civil money penalty.....	24
§ 160.406	Violations of an identical requirement or prohibition.....	24
§ 160.408	Factors considered in determining the amount of a civil money penalty.....	25
§ 160.410	Affirmative defenses.....	25
§ 160.412	Waiver.....	26
§ 160.414	Limitations.....	26
§ 160.416	Authority to settle.....	26
§ 160.418	Penalty not exclusive.....	26
§ 160.420	Notice of proposed determination.....	26
§ 160.422	Failure to request a hearing.....	26
§ 160.424	Collection of penalty.....	27
§ 160.426	Notification of the public and other agencies.....	27
<b>SUBPART E—PROCEDURES FOR HEARINGS .....</b>		<b>27</b>
§ 160.500	Applicability.....	27
§ 160.502	Definitions.....	27
§ 160.504	Hearing before an ALJ.....	27
§ 160.506	Rights of the parties.....	28
§ 160.508	Authority of the ALJ.....	28
§ 160.510	Ex parte contacts.....	29
§ 160.512	Prehearing conferences.....	29
§ 160.514	Authority to settle.....	29

§ 160.516	Discovery .....	29
§ 160.518	Exchange of witness lists, witness statements, and exhibits. ....	30
§ 160.520	Subpoenas for attendance at hearing. ....	30
§ 160.522	Fees.....	31
§ 160.524	Form, filing, and service of papers. ....	31
§ 160.526	Computation of time.....	31
§ 160.528	Motions. ....	31
§ 160.530	Sanctions.....	32
§ 160.532	Collateral estoppel. ....	32
§ 160.534	The hearing. ....	32
§ 160.536	Statistical sampling .....	33
§ 160.538	Witnesses. ....	33
§ 160.540	Evidence.....	33
§ 160.542	The record. ....	34
§ 160.544	Post hearing briefs. ....	34
§ 160.546	ALJ's decision. ....	34
§ 160.548	Appeal of the ALJ's decision.....	34
§ 160.550	Stay of the Secretary's decision. ....	35
 <b>PART 162—ADMINISTRATIVE REQUIREMENTS .....</b>		<b>37</b>
<b>SUBPART A—GENERAL PROVISIONS .....</b>		<b>38</b>
§ 162.100	Applicability.....	38
§ 162.103	Definitions.....	38
<b>SUBPARTS B-C [RESERVED] .....</b>		<b>39</b>
<b>SUBPART D—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH CARE PROVIDERS.....</b>		<b>39</b>
§ 162.402	[Reserved].....	39

§ 162.404	Compliance dates of the implementation of the standard unique health identifier for health care providers. ....	39
§ 162.406	Standard unique health identifier for health care providers. ....	39
§ 162.408	National Provider System. ....	39
§ 162.410	Implementation specifications: Health care providers. ....	40
§ 162.412	Implementation specifications: Health plans. ....	40
§ 162.414	Implementation specifications: Health care clearinghouses. ....	40
<b>SUBPART E—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH PLANS</b>		<b>40</b>
§ 162.502	[Reserved].....	40
§ 162.504	Compliance requirements for the implementation of the standard unique health plan identifier.....	40
§ 162.506	Standard unique health plan identifier.....	41
§ 162.508	Enumeration System.....	41
§ 162.510	Full implementation requirements: Covered entities. ....	41
§ 162.512	Implementation specifications: Health plans. ....	41
§ 162.514	Other entity identifier.....	42
<b>SUBPART F—STANDARD UNIQUE EMPLOYER IDENTIFIER</b>		<b>42</b>
§ 162.600	Compliance dates of the implementation of the standard unique employer identifier.....	42
§ 162.605	Standard unique employer identifier. ....	42
§ 162.610	Implementation specifications for covered entities.....	42
<b>SUBPARTS G-H [RESERVED]</b> .....		<b>42</b>
<b>SUBPART I—GENERAL PROVISIONS FOR TRANSACTIONS</b>		<b>42</b>
§ 162.900	[Reserved].....	42
§ 162.910	Maintenance of standards and adoption of modifications and new standards. ....	42
§ 162.915	Trading partner agreements.....	43
§ 162.920	Availability of implementation specifications and operating rules.....	43
§ 162.923	Requirements for covered entities. ....	46
§ 162.925	Additional requirements for health plans.....	47

§ 162.930	Additional rules for health care clearinghouses.....	47
§ 162.940	Exceptions from standards to permit testing of proposed modifications.....	48
<b>SUBPART J—CODE SETS.....</b>		<b>49</b>
§ 162.1000	General requirements.....	49
§ 162.1002	Medical data code sets.....	49
§ 162.1011	Valid code sets.....	50
<b>SUBPART K—HEALTH CARE CLAIMS OR EQUIVALENT ENCOUNTER INFORMATION.....</b>		<b>50</b>
§ 162.1101	Health care claims or equivalent encounter information transaction.....	50
§ 162.1102	Standards for health care claims or equivalent encounter information transaction.....	50
<b>SUBPART L—ELIGIBILITY FOR A HEALTH PLAN.....</b>		<b>52</b>
§ 162.1201	Eligibility for a health plan transaction.....	52
§ 162.1202	Standards for eligibility for a health plan transaction.....	52
§ 162.1203	Operating rules for eligibility for a health plan transaction.....	52
<b>SUBPART M—REFERRAL CERTIFICATION AND AUTHORIZATION.....</b>		<b>53</b>
§ 162.1301	Referral certification and authorization transaction.....	53
§ 162.1302	Standards for referral certification and authorization transaction.....	53
<b>SUBPART N—HEALTH CARE CLAIM STATUS.....</b>		<b>54</b>
§ 162.1401	Health care claim status transaction.....	54
§ 162.1402	Standards for health care claim status transaction.....	54
§ 162.1403	Operating rules for health care claim status transaction.....	54
<b>SUBPART O—ENROLLMENT AND DISENROLLMENT IN A HEALTH PLAN.....</b>		<b>54</b>
§ 162.1501	Enrollment and disenrollment in a health plan transaction.....	54
§ 162.1502	Standards for enrollment and disenrollment in a health plan transaction.....	54
<b>SUBPART P—HEALTH CARE ELECTRONIC FUNDS TRANSFERS (EFT) AND REMITTANCE ADVICE.....</b>		<b>55</b>
§ 162.1601	Health care electronic funds transfers (EFT) and remittance advice transaction.....	55

§ 162.1602	Standards for health care electronic funds transfers (EFT) and remittance advice transaction. ....	55
§ 162.1603	Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction. ....	56
<b>SUBPART Q—HEALTH PLAN PREMIUM PAYMENTS</b> .....		<b>56</b>
§ 162.1701	Health plan premium payments transaction. ....	56
§ 162.1702	Standards for health plan premium payments transaction. ....	56
<b>SUBPART R—COORDINATION OF BENEFITS</b> .....		<b>57</b>
§ 162.1801	Coordination of benefits transaction. ....	57
§ 162.1802	Standards for coordination of benefits information transaction. ....	57
<b>SUBPART S—MEDICAID PHARMACY SUBROGATION</b> .....		<b>58</b>
§ 162.1901	Medicaid pharmacy subrogation transaction.....	58
§ 162.1902	Standard for Medicaid pharmacy subrogation transaction.....	58
 <b>PART 164—SECURITY AND PRIVACY</b> .....		 <b>59</b>
<b>SUBPART A—GENERAL PROVISIONS</b> .....		<b>59</b>
§ 164.102	Statutory basis.....	59
§ 164.103	Definitions.....	59
§ 164.104	Applicability. ....	60
§ 164.105	Organizational requirements.....	60
§ 164.106	Relationship to other parts.....	62
<b>SUBPART B [RESERVED]</b> .....		<b>62</b>
<b>SUBPART C—SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION</b> .....		<b>62</b>
§ 164.302	Applicability. ....	62
§ 164.304	Definitions.....	62
§ 164.306	Security standards: General rules. ....	63
§ 164.308	Administrative safeguards. ....	64

§ 164.310 Physical safeguards.....	66
§ 164.312 Technical safeguards. ....	66
§ 164.314 Organizational requirements.....	67
§ 164.316 Policies and procedures and documentation requirements.....	68
§ 164.318 Compliance dates for the initial implementation of the security standards. ....	68
<b>SUBPART D—NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION.....</b>	<b>71</b>
§ 164.400 Applicability.....	71
§ 164.402 Definitions.....	71
§ 164.404 Notification to individuals.....	71
§ 164.406 Notification to the media. ....	72
§ 164.408 Notification to the Secretary. ....	72
§ 164.410 Notification by a business associate.....	73
§ 164.412 Law enforcement delay. ....	73
§ 164.414 Administrative requirements and burden of proof.....	73
<b>SUBPART E—PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.....</b>	<b>73</b>
§ 164.500 Applicability.....	73
§ 164.501 Definitions.....	74
§ 164.502 Uses and disclosures of protected health information: General rules. ....	77
§ 164.504 Uses and disclosures: Organizational requirements.....	81
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. ....	84
§ 164.508 Uses and disclosures for which an authorization is required.....	85
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.....	87
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required. ....	88
§ 164.514 Other requirements relating to uses and disclosures of protected health information.....	96
§ 164.520 Notice of privacy practices for protected health information. ....	101
§ 164.522 Rights to request privacy protection for protected health information. ....	104

**§ 164.524 Access of individuals to protected health information.....105**

**§ 164.526 Amendment of protected health information. ....108**

**§ 164.528 Accounting of disclosures of protected health information.....110**

**§ 164.530 Administrative requirements.....111**

**§ 164.532 Transition provisions. ....114**

**§ 164.534 Compliance dates for initial implementation of the privacy standards. ....115**



---

**PART 160—GENERAL  
ADMINISTRATIVE  
REQUIREMENTS**

---

**Contents**

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.  
§ 160.102 Applicability.  
§ 160.103 Definitions.  
§ 160.104 Modifications.  
§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

Subpart B—Preemption of State Law

§ 160.201 Statutory basis.  
§ 160.202 Definitions.  
§ 160.203 General rule and exceptions.  
§ 160.204 Process for requesting exception determinations.  
§ 160.205 Duration of effectiveness of exception determinations.

Subpart C—Compliance and Investigations

§ 160.300 Applicability.  
§ 160.302 [Reserved]  
§ 160.304 Principles for achieving compliance.  
§ 160.306 Complaints to the Secretary.  
§ 160.308 Compliance reviews.  
§ 160.310 Responsibilities of covered entities and business associates.  
§ 160.312 Secretarial action regarding complaints and compliance reviews.  
§ 160.314 Investigational subpoenas and inquiries.

§ 160.316 Refraining from intimidation or retaliation.

Subpart D—Imposition of Civil Money Penalties

§ 160.400 Applicability.  
§ 160.401 Definitions.  
§ 160.402 Basis for a civil money penalty.  
§ 160.404 Amount of a civil money penalty.  
§ 160.406 Violations of an identical requirement or prohibition.  
§ 160.408 Factors considered in determining the amount of a civil money penalty.  
§ 160.410 Affirmative defenses.  
§ 160.412 Waiver.  
§ 160.414 Limitations.  
§ 160.416 Authority to settle.  
§ 160.418 Penalty not exclusive.  
§ 160.420 Notice of proposed determination.  
§ 160.422 Failure to request a hearing.  
§ 160.424 Collection of penalty.  
§ 160.426 Notification of the public and other agencies.

Subpart E—Procedures for Hearings

§ 160.500 Applicability.  
§ 160.502 Definitions.  
§ 160.504 Hearing before an ALJ.  
§ 160.506 Rights of the parties.  
§ 160.508 Authority of the ALJ.  
§ 160.510 Ex parte contacts.  
§ 160.512 Prehearing conferences.  
§ 160.514 Authority to settle.  
§ 160.516 Discovery.  
§ 160.518 Exchange of witness lists, witness statements, and exhibits.  
§ 160.520 Subpoenas for attendance at hearing.

§ 160.522 Fees.  
§ 160.524 Form, filing, and service of papers.  
§ 160.526 Computation of time.  
§ 160.528 Motions.  
§ 160.530 Sanctions.  
§ 160.532 Collateral estoppel.  
§ 160.534 The hearing.  
§ 160.536 Statistical sampling.  
§ 160.538 Witnesses.  
§ 160.540 Evidence.  
§ 160.542 The record.  
§ 160.544 Post hearing briefs.  
§ 160.546 ALJ's decision.  
§ 160.548 Appeal of the ALJ's decision.  
§ 160.550 Stay of the Secretary's decision.  
§ 160.552 Harmless error.

---

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); 5 U.S.C. 552; secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279; and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.

SOURCE: 65 FR 82798, Dec. 28, 2000, unless otherwise noted.

**Subpart A—General Provisions**

**§ 160.101 Statutory basis and purpose.**

The requirements of this subchapter implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

[78 FR 5687, Jan. 25, 2013]

**§ 160.102 Applicability.**

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

**§ 160.103 Definitions.**

Except as otherwise provided, the following definitions apply to this subchapter:

*Act* means the Social Security Act.

*Administrative simplification provision* means any

requirement or prohibition established by:

- (1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;
- (2) Section 264 of Pub. L. 104-191;
- (3) Sections 13400-13424 of Public Law 111-5; or
- (4) This subchapter.

*ALJ* means Administrative Law Judge.

*ANSI* stands for the American National Standards Institute.

*Business associate:* (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in

§ 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance

issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

*Civil money penalty or penalty* means the amount determined under § 160.404 of this part and includes the plural of these terms.

*CMS* stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

*Compliance date* means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

*Covered entity* means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

*Disclosure* means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

*EIN* stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

- (1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
- (2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

*Electronic media* means:

- (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as

magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

*Electronic protected health information* means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of *protected health information* as specified in this section.

*Employer* is defined as it is in 26 U.S.C. 3401(d).

*Family member* means, with respect to an individual:

- (1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
- (2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one

parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

*Genetic information* means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

*Genetic services* means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

*Genetic test* means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

*Group health plan* (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance,

reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

*HHS* stands for the Department of Health and Human Services.

*Health care* means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

*Health care clearinghouse* means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data

elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

*Health care provider* means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

*Health information* means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

*Health insurance issuer* (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the

business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

*Health maintenance organization (HMO)* (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

*Health plan* means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

*Implementation specification* means specific requirements or instructions for implementing a standard.

*Individual* means the person who is the subject of protected health information.

*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan,

employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

*Manifestation or manifested* means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

*Modify or modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

*Organized health care arrangement* means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than

one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

*Person* means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

*Protected health information* means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

*Respondent* means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

*Secretary* means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

*Small health plan* means a health plan with annual receipts of \$5 million or less.

*Standard* means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

*Standard setting organization (SSO)* means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

*State* refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

*Subcontractor* means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

*Trading partner agreement* means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

*Transaction* means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

not they are paid by the covered entity or business associate.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

(3) Coordination of benefits.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002; 67 FR 53266, Aug. 14, 2002; 68 FR 8374, Feb. 20, 2003; 71 FR 8424, Feb. 16, 2006; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 78 FR 5687, Jan. 25, 2013]

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002]

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

**§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.**

(7) Health plan premium payments.

**§ 160.104 Modifications.**

(8) Referral certification and authorization.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.

(9) First report of injury.

(10) Health claims attachments.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

[78 FR 5689, Jan. 25, 2013]

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

**Subpart B—Preemption of State Law**

*Use* means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

**§ 160.201 Statutory basis.**

*Violation* or *violate* means, as the context may require, failure to comply with an administrative simplification provision.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.

*Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

[78 FR 5689, Jan. 25, 2013]



**§ 160.202 Definitions.**

For purposes of this subpart, the following terms have the following meanings:

*Contrary*, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

*More stringent* means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

*Relates to the privacy of individually identifiable health information* means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

*State law* means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 74 FR 42767, Aug. 24, 2009; 78 FR 5689, Jan. 25, 2013]

**§ 160.203 General rule and exceptions.**

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]

#### **§ 160.204 Process for requesting exception determinations.**

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the FEDERAL REGISTER. Until the Secretary's determination is made, the standard, requirement,

or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

#### **§ 160.205 Duration of effectiveness of exception determinations.**

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

#### **Subpart C—Compliance and Investigations**

SOURCE: 71 FR 8424, Feb. 16, 2006, unless otherwise noted.

#### **§ 160.300 Applicability.**

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

[78 FR 5690, Jan. 25, 2013]

**§ 160.302 [Reserved]**

**§ 160.304 Principles for achieving compliance.**

(a) *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

[78 FR 5690, Jan. 25, 2013]

**§ 160.306 Complaints to the Secretary.**

(a) *Right to file a complaint.* A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the FEDERAL REGISTER.

(c) *Investigation.* (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

[71 FR 8424, Feb. 16, 2006, as amended at 78 FR 5690, Jan. 25, 2013]

**§ 160.308 Compliance reviews.**

(a) The Secretary will conduct a compliance review to determine

whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

[78 FR 5690, Jan. 25, 2013]

**§ 160.310 Responsibilities of covered entities and business associates.**

(a) *Provide records and compliance reports.* A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

*(c) Permit access to information.*

(1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

[78 FR 5690, Jan. 25, 2013]

**§ 160.312 Secretarial action regarding complaints and compliance reviews.**

*(a) Resolution when noncompliance is indicated.* (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of

such finding in a notice of proposed determination in accordance with § 160.420 of this part.

*(b) Resolution when no violation is found.* If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

[78 FR 5690, Jan. 25, 2013]

**§ 160.314 Investigational subpoenas and inquiries.**

(a) The Secretary may issue subpoenas in accordance with 42 U.S.C. 405(d) and (e), 1320a-7a(j), and 1320d-5 to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review pursuant to this part. For purposes of this paragraph, a person other than a natural person is termed an “entity.”

(1) A subpoena issued under this paragraph must—

(i) State the name of the person (including the entity, if applicable) to whom the subpoena is addressed;

(ii) State the statutory authority for the subpoena;

(iii) Indicate the date, time, and place that the testimony will take place;

(iv) Include a reasonably specific description of any

documents or items required to be produced; and

(v) If the subpoena is addressed to an entity, describe with reasonable particularity the subject matter on which testimony is required. In that event, the entity must designate one or more natural persons who will testify on its behalf, and must state as to each such person that person's name and address and the matters on which he or she will testify. The designated person must testify as to matters known or reasonably available to the entity.

(2) A subpoena under this section must be served by—

(i) Delivering a copy to the natural person named in the subpoena or to the entity named in the subpoena at its last principal place of business; or

(ii) Registered or certified mail addressed to the natural person at his or her last known dwelling place or to the entity at its last known principal place of business.

(3) A verified return by the natural person serving the subpoena setting forth the manner of service or, in the case of service by registered or certified mail, the signed return post office receipt, constitutes proof of service.

(4) Witnesses are entitled to the same fees and mileage as witnesses in the district courts of the United States (28 U.S.C. 1821 and 1825). Fees need not be paid at the time the subpoena is served.

(5) A subpoena under this section is enforceable through the district court of the United States for the district where the subpoenaed natural person resides or is found or where the entity transacts business.

(b) Investigational inquiries are non-public investigational proceedings conducted by the Secretary.

(1) Testimony at investigational inquiries will be taken under oath or affirmation.

(2) Attendance of non-witnesses is discretionary with the Secretary, except that a witness is entitled to be accompanied, represented, and advised by an attorney.

(3) Representatives of the Secretary are entitled to attend and ask questions.

(4) A witness will have the opportunity to clarify his or her answers on the record following questioning by the Secretary.

(5) Any claim of privilege must be asserted by the witness on the record.

(6) Objections must be asserted on the record. Errors of any kind that might be corrected if promptly presented will be deemed to be waived unless reasonable objection is made at the investigational inquiry. Except where the objection is on the grounds of privilege, the question will be answered on the record, subject to objection.

(7) If a witness refuses to answer any question not privileged or to produce requested documents or items, or engages in conduct likely to

delay or obstruct the investigational inquiry, the Secretary may seek enforcement of the subpoena under paragraph (a)(5) of this section.

(8) The proceedings will be recorded and transcribed. The witness is entitled to a copy of the transcript, upon payment of prescribed costs, except that, for good cause, the witness may be limited to inspection of the official transcript of his or her testimony.

(9)(i) The transcript will be submitted to the witness for signature.

(A) Where the witness will be provided a copy of the transcript, the transcript will be submitted to the witness for signature. The witness may submit to the Secretary written proposed corrections to the transcript, with such corrections attached to the transcript. If the witness does not return a signed copy of the transcript or proposed corrections within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of its being submitted to him or her for signature, the witness will be deemed to have agreed that the transcript is true and accurate.

(B) Where, as provided in paragraph (b)(8) of this section, the witness is limited to inspecting the transcript, the witness will have the opportunity at the time of inspection to propose corrections to the transcript, with corrections attached to the transcript. The witness will also have the opportunity to sign the transcript. If the witness does not sign the transcript or offer corrections within 30 days (computed in the same manner

as prescribed under § 160.526 of this part) of receipt of notice of the opportunity to inspect the transcript, the witness will be deemed to have agreed that the transcript is true and accurate.

(ii) The Secretary's proposed corrections to the record of transcript will be attached to the transcript.

(c) Consistent with § 160.310(c)(3), testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in any administrative or judicial proceeding.

#### **§ 160.316 Refraining from intimidation or retaliation.**

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

(a) Filing of a complaint under § 160.306;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part; or

(c) Opposing any act or practice made unlawful by this subchapter, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of subpart E of part 164 of this subchapter.

[71 FR 8426, Feb. 16, 2006, as amended at 78 FR 5691, Jan. 25, 2013]

#### **Subpart D—Imposition of Civil Money Penalties**

SOURCE: 71 FR 8426, Feb. 16, 2006, unless otherwise noted.

#### **§ 160.400 Applicability.**

This subpart applies to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

#### **§ 160.401 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

*Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

*Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[74 FR 56130, Oct. 30, 2009, as amended at 78 FR 5691, Jan. 25, 2013]

#### **§ 160.402 Basis for a civil money penalty.**

(a) *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) *Violation by more than one covered entity or business associate.* (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) *Violation attributed to a covered entity or business associate.* (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

[78 FR 5691, Jan. 25, 2013]

**§ 160.404 Amount of a civil money penalty.**

(a) The amount of a civil money penalty will be determined in accordance with paragraph (b) of this section and §§ 160.406, 160.408, and 160.412.

(b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

(1) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty—

(i) In the amount of more than \$100 for each violation; or

(ii) In excess of \$25,000 for identical violations during a calendar year (January 1 through the following December 31);

(2) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty—

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

(A) In the amount of less than \$100 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,

(A) In the amount of less than \$1,000 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than \$10,000 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would

have known that the violation occurred,

(A) In the amount of less than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

(3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56130, Oct. 30, 2009; 78 FR 5691, Jan. 25, 2013]

**§ 160.406 Violations of an identical requirement or prohibition.**

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

[78 FR 5691, Jan. 25, 2013]

**§ 160.408 Factors considered in determining the amount of a civil money penalty.**

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar

to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

[78 FR 5691, Jan. 25, 2013]

**§ 160.410 Affirmative defenses.**

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on

a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d-6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:



(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

[78 FR 5692, Jan. 25, 2013]

**§ 160.412 Waiver.**

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the

payment of the penalty would be excessive relative to the violation.

[8 FR 5692, Jan. 25, 2013]

**§ 160.414 Limitations.**

No action under this subpart may be entertained unless commenced by the Secretary, in accordance with § 160.420, within 6 years from the date of the occurrence of the violation.

**§ 160.416 Authority to settle.**

Nothing in this subpart limits the authority of the Secretary to settle any issue or case or to compromise any penalty.

**§ 160.418 Penalty not exclusive.**

Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1) and 42 U.S.C. 299b-22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

[78 FR 5692, Jan. 25, 2013]

**§ 160.420 Notice of proposed determination.**

(a) If a penalty is proposed in accordance with this part, the Secretary must deliver, or send by certified mail with return receipt requested, to the respondent, written notice of the Secretary's intent to impose a penalty. This notice of proposed determination must include—

(1) Reference to the statutory basis for the penalty;

(2) A description of the findings of fact regarding the violations with respect to which the

penalty is proposed (except that, in any case where the Secretary is relying upon a statistical sampling study in accordance with § 160.536 of this part, the notice must provide a copy of the study relied upon by the Secretary);

(3) The reason(s) why the violation(s) subject(s) the respondent to a penalty;

(4) The amount of the proposed penalty and a reference to the subparagraph of § 160.404 upon which it is based.

(5) Any circumstances described in § 160.408 that were considered in determining the amount of the proposed penalty; and

(6) Instructions for responding to the notice, including a statement of the respondent's right to a hearing, a statement that failure to request a hearing within 90 days permits the imposition of the proposed penalty without the right to a hearing under § 160.504 or a right of appeal under § 160.548 of this part, and the address to which the hearing request must be sent.

(b) The respondent may request a hearing before an ALJ on the proposed penalty by filing a request in accordance with § 160.504 of this part.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56131, Oct. 30, 2009]

**§ 160.422 Failure to request a hearing.**

If the respondent does not request a hearing within the time prescribed by § 160.504 of this

part and the matter is not settled pursuant to § 160.416, the Secretary will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5. The Secretary will notify the respondent by certified mail, return receipt requested, of any penalty that has been imposed and of the means by which the respondent may satisfy the penalty, and the penalty is final on receipt of the notice. The respondent has no right to appeal a penalty under § 160.548 of this part with respect to which the respondent has not timely requested a hearing.

**§ 160.424 Collection of penalty.**

(a) Once a determination of the Secretary to impose a penalty has become final, the penalty will be collected by the Secretary, subject to the first sentence of 42 U.S.C. 1320a-7a(f).

(b) The penalty may be recovered in a civil action brought in the United States district court for the district where the respondent resides, is found, or is located.

(c) The amount of a penalty, when finally determined, or the amount agreed upon in compromise, may be deducted from any sum then or later owing by the United States, or by a State agency, to the respondent.

(d) Matters that were raised or that could have been raised in a hearing before an ALJ, or in an appeal under 42 U.S.C. 1320a-7a(e), may not be raised as a defense in a civil action by the United States to collect a penalty under this part.

**§ 160.426 Notification of the public and other agencies.**

Whenever a proposed penalty becomes final, the Secretary will notify, in such manner as the Secretary deems appropriate, the public and the following organizations and entities thereof and the reason it was imposed: the appropriate State or local medical or professional organization, the appropriate State agency or agencies administering or supervising the administration of State health care programs (as defined in 42 U.S.C. 1320a-7(h)), the appropriate utilization and quality control peer review organization, and the appropriate State or local licensing agency or organization (including the agency specified in 42 U.S.C. 1395aa(a), 1396a(a)(33)).

**Subpart E—Procedures for Hearings**

SOURCE: 71 FR 8428, Feb. 16, 2006, unless otherwise noted.

**§ 160.500 Applicability.**

This subpart applies to hearings conducted relating to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

**§ 160.502 Definitions.**

As used in this subpart, the following term has the following meaning:

*Board* means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three.

**§ 160.504 Hearing before an ALJ.**

(a) A respondent may request a hearing before an ALJ. The parties to the hearing proceeding consist of—

(1) The respondent; and

(2) The officer(s) or employee(s) of HHS to whom the enforcement authority involved has been delegated.

(b) The request for a hearing must be made in writing signed by the respondent or by the respondent's attorney and sent by certified mail, return receipt requested, to the address specified in the notice of proposed determination. The request for a hearing must be mailed within 90 days after notice of the proposed determination is received by the respondent. For purposes of this section, the respondent's date of receipt of the notice of proposed determination is presumed to be 5 days after the date of the notice unless the respondent makes a reasonable showing to the contrary to the ALJ.

(c) The request for a hearing must clearly and directly admit, deny, or explain each of the findings of fact contained in the notice of proposed determination with regard to which the respondent has any knowledge. If the respondent has no knowledge of a particular finding of fact and so states, the finding shall be deemed denied. The request for a hearing must also state the circumstances or arguments that the respondent alleges constitute the grounds for any defense and the factual and legal basis for opposing the penalty, except that a respondent may raise an affirmative defense

under § 160.410(b)(1) at any time.

(d) The ALJ must dismiss a hearing request where—

(1) On motion of the Secretary, the ALJ determines that the respondent's hearing request is not timely filed as required by paragraphs (b) or does not meet the requirements of paragraph (c) of this section;

(2) The respondent withdraws the request for a hearing;

(3) The respondent abandons the request for a hearing; or

(4) The respondent's hearing request fails to raise any issue that may properly be addressed in a hearing.

**§ 160.506 Rights of the parties.**

(a) Except as otherwise limited by this subpart, each party may—

(1) Be accompanied, represented, and advised by an attorney;

(2) Participate in any conference held by the ALJ;

(3) Conduct discovery of documents as permitted by this subpart;

(4) Agree to stipulations of fact or law that will be made part of the record;

(5) Present evidence relevant to the issues at the hearing;

(6) Present and cross-examine witnesses;

(7) Present oral arguments at the hearing as permitted by the ALJ; and

(8) Submit written briefs and proposed findings of fact and conclusions of law after the hearing.

(b) A party may appear in person or by a representative. Natural persons who appear as an attorney or other representative must conform to the standards of conduct and ethics required of practitioners before the courts of the United States.

(c) Fees for any services performed on behalf of a party by an attorney are not subject to the provisions of 42 U.S.C. 406, which authorizes the Secretary to specify or limit their fees.

**§ 160.508 Authority of the ALJ.**

(a) The ALJ must conduct a fair and impartial hearing, avoid delay, maintain order, and ensure that a record of the proceeding is made.

(b) The ALJ may—

(1) Set and change the date, time and place of the hearing upon reasonable notice to the parties;

(2) Continue or recess the hearing in whole or in part for a reasonable period of time;

(3) Hold conferences to identify or simplify the issues, or to consider other matters that may aid in the expeditious disposition of the proceeding;

(4) Administer oaths and affirmations;

(5) Issue subpoenas requiring the attendance of witnesses at hearings and the production of documents at or in relation to hearings;

(6) Rule on motions and other procedural matters;

(7) Regulate the scope and timing of documentary discovery as permitted by this subpart;

(8) Regulate the course of the hearing and the conduct of representatives, parties, and witnesses;

(9) Examine witnesses;

(10) Receive, rule on, exclude, or limit evidence;

(11) Upon motion of a party, take official notice of facts;

(12) Conduct any conference, argument or hearing in person or, upon agreement of the parties, by telephone; and

(13) Upon motion of a party, decide cases, in whole or in part, by summary judgment where there is no disputed issue of material fact. A summary judgment decision constitutes a hearing on the record for the purposes of this subpart.

(c) The ALJ—

(1) May not find invalid or refuse to follow Federal statutes, regulations, or Secretarial delegations of authority and must give deference to published guidance to the extent not inconsistent with statute or regulation;

(2) May not enter an order in the nature of a directed verdict;

(3) May not compel settlement negotiations;

(4) May not enjoin any act of the Secretary; or

(5) May not review the exercise of discretion by the Secretary with respect to whether to grant an extension under § 160.410(b)(2)(ii)(B) or (c)(2)(ii) of this part or to provide technical assistance under 42 U.S.C. 1320d-5(b)(2)(B).

**§ 160.510 Ex parte contacts.**

No party or person (except employees of the ALJ's office) may communicate in any way with the ALJ on any matter at issue in a case, unless on notice and opportunity for both parties to participate. This provision does not prohibit a party or person from inquiring about the status of a case or asking routine questions concerning administrative functions or procedures.

**§ 160.512 Prehearing conferences.**

(a) The ALJ must schedule at least one prehearing conference, and may schedule additional prehearing conferences as appropriate, upon reasonable notice, which may not be less than 14 business days, to the parties.

(b) The ALJ may use prehearing conferences to discuss the following—

(1) Simplification of the issues;

(2) The necessity or desirability of amendments to the pleadings, including the need for a more definite statement;

(3) Stipulations and admissions of fact or as to the contents and authenticity of documents;

(4) Whether the parties can agree to submission of the case on a stipulated record;

(5) Whether a party chooses to waive appearance at an oral hearing and to submit only documentary evidence (subject to the objection of the other party) and written argument;

(6) Limitation of the number of witnesses;

(7) Scheduling dates for the exchange of witness lists and of proposed exhibits;

(8) Discovery of documents as permitted by this subpart;

(9) The time and place for the hearing;

(10) The potential for the settlement of the case by the parties; and

(11) Other matters as may tend to encourage the fair, just and expeditious disposition of the proceedings, including the protection of privacy of individually identifiable health information that may be submitted into evidence or otherwise used in the proceeding, if appropriate.

(c) The ALJ must issue an order containing the matters agreed upon by the parties or ordered by the ALJ at a prehearing conference.

**§ 160.514 Authority to settle.**

The Secretary has exclusive authority to settle any issue or case without the consent of the ALJ.

**§ 160.516 Discovery.**

(a) A party may make a request to another party for production of documents for inspection and copying that are relevant and material to the issues before the ALJ.

(b) For the purpose of this section, the term “documents” includes information, reports, answers, records, accounts, papers and other data and documentary evidence. Nothing contained in this section may be interpreted to require the creation of a document, except that requested data stored in an electronic data storage system must be produced in a form accessible to the requesting party.

(c) Requests for documents, requests for admissions, written interrogatories, depositions and any forms of discovery, other than those permitted under paragraph (a) of this section, are not authorized.

(d) This section may not be construed to require the disclosure of interview reports or statements obtained by any party, or on behalf of any party, of persons who will not be called as witnesses by that party, or analyses and summaries prepared in conjunction with the investigation or litigation of the case, or any otherwise privileged documents.

(e)(1) When a request for production of documents has

been received, within 30 days the party receiving that request must either fully respond to the request, or state that the request is being objected to and the reasons for that objection. If objection is made to part of an item or category, the part must be specified. Upon receiving any objections, the party seeking production may then, within 30 days or any other time frame set by the ALJ, file a motion for an order compelling discovery. The party receiving a request for production may also file a motion for protective order any time before the date the production is due.

(2) The ALJ may grant a motion for protective order or deny a motion for an order compelling discovery if the ALJ finds that the discovery sought—

(i) Is irrelevant;

(ii) Is unduly costly or burdensome;

(iii) Will unduly delay the proceeding; or

(iv) Seeks privileged information.

(3) The ALJ may extend any of the time frames set forth in paragraph (e)(1) of this section.

(4) The burden of showing that discovery should be allowed is on the party seeking discovery.

**§ 160.518 Exchange of witness lists, witness statements, and exhibits.**

(a) The parties must exchange witness lists, copies of prior written statements of proposed witnesses, and copies of proposed hearing exhibits,

including copies of any written statements that the party intends to offer in lieu of live testimony in accordance with § 160.538, not more than 60, and not less than 15, days before the scheduled hearing, except that if a respondent intends to introduce the evidence of a statistical expert, the respondent must provide the Secretarial party with a copy of the statistical expert's report not less than 30 days before the scheduled hearing.

(b)(1) If, at any time, a party objects to the proposed admission of evidence not exchanged in accordance with paragraph (a) of this section, the ALJ must determine whether the failure to comply with paragraph (a) of this section should result in the exclusion of that evidence.

(2) Unless the ALJ finds that extraordinary circumstances justified the failure timely to exchange the information listed under paragraph (a) of this section, the ALJ must exclude from the party's case-in-chief—

(i) The testimony of any witness whose name does not appear on the witness list; and

(ii) Any exhibit not provided to the opposing party as specified in paragraph (a) of this section.

(3) If the ALJ finds that extraordinary circumstances existed, the ALJ must then determine whether the admission of that evidence would cause substantial prejudice to the objecting party.

(i) If the ALJ finds that there is no substantial prejudice, the evidence may be admitted.

(ii) If the ALJ finds that there is substantial prejudice, the ALJ may exclude the evidence, or, if he or she does not exclude the evidence, must postpone the hearing for such time as is necessary for the objecting party to prepare and respond to the evidence, unless the objecting party waives postponement.

(c) Unless the other party objects within a reasonable period of time before the hearing, documents exchanged in accordance with paragraph (a) of this section will be deemed to be authentic for the purpose of admissibility at the hearing.

**§ 160.520 Subpoenas for attendance at hearing.**

(a) A party wishing to procure the appearance and testimony of any person at the hearing may make a motion requesting the ALJ to issue a subpoena if the appearance and testimony are reasonably necessary for the presentation of a party's case.

(b) A subpoena requiring the attendance of a person in accordance with paragraph (a) of this section may also require the person (whether or not the person is a party) to produce relevant and material evidence at or before the hearing.

(c) When a subpoena is served by a respondent on a particular employee or official or particular office of HHS, the Secretary may comply by designating any knowledgeable HHS representative to appear and testify.

(d) A party seeking a subpoena must file a written motion not less than 30 days before the date fixed for the hearing, unless otherwise allowed by the ALJ

for good cause shown. That motion must—

- (1) Specify any evidence to be produced;
- (2) Designate the witnesses; and
- (3) Describe the address and location with sufficient particularity to permit those witnesses to be found.

(e) The subpoena must specify the time and place at which the witness is to appear and any evidence the witness is to produce.

(f) Within 15 days after the written motion requesting issuance of a subpoena is served, any party may file an opposition or other response.

(g) If the motion requesting issuance of a subpoena is granted, the party seeking the subpoena must serve it by delivery to the person named, or by certified mail addressed to that person at the person's last dwelling place or principal place of business.

(h) The person to whom the subpoena is directed may file with the ALJ a motion to quash the subpoena within 10 days after service.

(i) The exclusive remedy for contumacy by, or refusal to obey a subpoena duly served upon, any person is specified in 42 U.S.C. 405(e).

#### **§ 160.522 Fees.**

The party requesting a subpoena must pay the cost of the fees and mileage of any witness subpoenaed in the amounts that would be payable to a witness in

a proceeding in United States District Court. A check for witness fees and mileage must accompany the subpoena when served, except that, when a subpoena is issued on behalf of the Secretary, a check for witness fees and mileage need not accompany the subpoena.

#### **§ 160.524 Form, filing, and service of papers.**

(a) *Forms.* (1) Unless the ALJ directs the parties to do otherwise, documents filed with the ALJ must include an original and two copies.

(2) Every pleading and paper filed in the proceeding must contain a caption setting forth the title of the action, the case number, and a designation of the paper, such as motion to quash subpoena.

(3) Every pleading and paper must be signed by and must contain the address and telephone number of the party or the person on whose behalf the paper was filed, or his or her representative.

(4) Papers are considered filed when they are mailed.

(b) *Service.* A party filing a document with the ALJ or the Board must, at the time of filing, serve a copy of the document on the other party. Service upon any party of any document must be made by delivering a copy, or placing a copy of the document in the United States mail, postage prepaid and addressed, or with a private delivery service, to the party's last known address. When a party is represented by an attorney, service must be made upon the attorney in lieu of the party.

(c) *Proof of service.* A certificate of the natural person serving the document by personal delivery or by mail, setting forth the manner of service, constitutes proof of service.

#### **§ 160.526 Computation of time.**

(a) In computing any period of time under this subpart or in an order issued thereunder, the time begins with the day following the act, event or default, and includes the last day of the period unless it is a Saturday, Sunday, or legal holiday observed by the Federal Government, in which event it includes the next business day.

(b) When the period of time allowed is less than 7 days, intermediate Saturdays, Sundays, and legal holidays observed by the Federal Government must be excluded from the computation.

(c) Where a document has been served or issued by placing it in the mail, an additional 5 days must be added to the time permitted for any response. This paragraph does not apply to requests for hearing under § 160.504.

#### **§ 160.528 Motions.**

(a) An application to the ALJ for an order or ruling must be by motion. Motions must state the relief sought, the authority relied upon and the facts alleged, and must be filed with the ALJ and served on all other parties.

(b) Except for motions made during a prehearing conference or at the hearing, all motions must be in writing. The ALJ

may require that oral motions be reduced to writing.

(c) Within 10 days after a written motion is served, or such other time as may be fixed by the ALJ, any party may file a response to the motion.

(d) The ALJ may not grant a written motion before the time for filing responses has expired, except upon consent of the parties or following a hearing on the motion, but may overrule or deny the motion without awaiting a response.

(e) The ALJ must make a reasonable effort to dispose of all outstanding motions before the beginning of the hearing.

#### **§ 160.530 Sanctions.**

The ALJ may sanction a person, including any party or attorney, for failing to comply with an order or procedure, for failing to defend an action or for other misconduct that interferes with the speedy, orderly or fair conduct of the hearing. The sanctions must reasonably relate to the severity and nature of the failure or misconduct. The sanctions may include—

(a) In the case of refusal to provide or permit discovery under the terms of this part, drawing negative factual inferences or treating the refusal as an admission by deeming the matter, or certain facts, to be established;

(b) Prohibiting a party from introducing certain evidence or otherwise supporting a particular claim or defense;

(c) Striking pleadings, in whole or in part;

(d) Staying the proceedings;

(e) Dismissal of the action;

(f) Entering a decision by default;

(g) Ordering the party or attorney to pay the attorney's fees and other costs caused by the failure or misconduct; and

(h) Refusing to consider any motion or other action that is not filed in a timely manner.

#### **§ 160.532 Collateral estoppel.**

When a final determination that the respondent violated an administrative simplification provision has been rendered in any proceeding in which the respondent was a party and had an opportunity to be heard, the respondent is bound by that determination in any proceeding under this part.

#### **§ 160.534 The hearing.**

(a) The ALJ must conduct a hearing on the record in order to determine whether the respondent should be found liable under this part.

(b) (1) The respondent has the burden of going forward and the burden of persuasion with respect to any:

(i) Affirmative defense pursuant to § 160.410 of this part;

(ii) Challenge to the amount of a proposed penalty pursuant to §§ 160.404-160.408 of this part, including any factors raised as mitigating factors; or

(iii) Claim that a proposed penalty should be reduced or

waived pursuant to § 160.412 of this part; and

(iv) Compliance with subpart D of part 164, as provided under § 164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

(3) The burden of persuasion will be judged by a preponderance of the evidence.

(c) The hearing must be open to the public unless otherwise ordered by the ALJ for good cause shown.

(d)(1) Subject to the 15-day rule under § 160.518(a) and the admissibility of evidence under § 160.540, either party may introduce, during its case in chief, items or information that arose or became known after the date of the issuance of the notice of proposed determination or the request for hearing, as applicable. Such items and information may not be admitted into evidence, if introduced—

(i) By the Secretary, unless they are material and relevant to the acts or omissions with respect to which the penalty is proposed in the notice of proposed determination pursuant to § 160.420 of this part, including circumstances that may increase penalties; or

(ii) By the respondent, unless they are material and relevant to an admission, denial or

explanation of a finding of fact in the notice of proposed determination under § 160.420 of this part, or to a specific circumstance or argument expressly stated in the request for hearing under § 160.504, including circumstances that may reduce penalties.

(2) After both parties have presented their cases, evidence may be admitted in rebuttal even if not previously exchanged in accordance with § 160.518.

[71 FR 8428, Feb. 16, 2006, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5692, Jan. 25, 2013]

**§ 160.536 Statistical sampling.**

(a) In meeting the burden of proof set forth in § 160.534, the Secretary may introduce the results of a statistical sampling study as evidence of the number of violations under § 160.406 of this part, or the factors considered in determining the amount of the civil money penalty under § 160.408 of this part. Such statistical sampling study, if based upon an appropriate sampling and computed by valid statistical methods, constitutes prima facie evidence of the number of violations and the existence of factors material to the proposed civil money penalty as described in §§ 160.406 and 160.408.

(b) Once the Secretary has made a prima facie case, as described in paragraph (a) of this section, the burden of going forward shifts to the respondent to produce evidence reasonably calculated to rebut the findings of the statistical sampling study. The Secretary will then be given

the opportunity to rebut this evidence.

**§ 160.538 Witnesses.**

(a) Except as provided in paragraph (b) of this section, testimony at the hearing must be given orally by witnesses under oath or affirmation.

(b) At the discretion of the ALJ, testimony of witnesses other than the testimony of expert witnesses may be admitted in the form of a written statement. The ALJ may, at his or her discretion, admit prior sworn testimony of experts that has been subject to adverse examination, such as a deposition or trial testimony. Any such written statement must be provided to the other party, along with the last known address of the witness, in a manner that allows sufficient time for the other party to subpoena the witness for cross-examination at the hearing. Prior written statements of witnesses proposed to testify at the hearing must be exchanged as provided in § 160.518.

(c) The ALJ must exercise reasonable control over the mode and order of interrogating witnesses and presenting evidence so as to:

(1) Make the interrogation and presentation effective for the ascertainment of the truth;

(2) Avoid repetition or needless consumption of time; and

(3) Protect witnesses from harassment or undue embarrassment.

(d) The ALJ must permit the parties to conduct cross-

examination of witnesses as may be required for a full and true disclosure of the facts.

(e) The ALJ may order witnesses excluded so that they cannot hear the testimony of other witnesses, except that the ALJ may not order to be excluded—

(1) A party who is a natural person;

(2) In the case of a party that is not a natural person, the officer or employee of the party appearing for the entity pro se or designated as the party's representative; or

(3) A natural person whose presence is shown by a party to be essential to the presentation of its case, including a person engaged in assisting the attorney for the Secretary.

**§ 160.540 Evidence.**

(a) The ALJ must determine the admissibility of evidence.

(b) Except as provided in this subpart, the ALJ is not bound by the Federal Rules of Evidence. However, the ALJ may apply the Federal Rules of Evidence where appropriate, for example, to exclude unreliable evidence.

(c) The ALJ must exclude irrelevant or immaterial evidence.

(d) Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or by considerations of undue delay or needless presentation of cumulative evidence.



(e) Although relevant, evidence must be excluded if it is privileged under Federal law.

(f) Evidence concerning offers of compromise or settlement are inadmissible to the extent provided in Rule 408 of the Federal Rules of Evidence.

(g) Evidence of crimes, wrongs, or acts other than those at issue in the instant case is admissible in order to show motive, opportunity, intent, knowledge, preparation, identity, lack of mistake, or existence of a scheme. This evidence is admissible regardless of whether the crimes, wrongs, or acts occurred during the statute of limitations period applicable to the acts or omissions that constitute the basis for liability in the case and regardless of whether they were referenced in the Secretary's notice of proposed determination under § 160.420 of this part.

(h) The ALJ must permit the parties to introduce rebuttal witnesses and evidence.

(i) All documents and other evidence offered or taken for the record must be open to examination by both parties, unless otherwise ordered by the ALJ for good cause shown.

**§ 160.542 The record.**

(a) The hearing must be recorded and transcribed. Transcripts may be obtained following the hearing from the ALJ. A party that requests a transcript of hearing proceedings must pay the cost of preparing the transcript unless, for good cause shown by the party, the payment is waived by the ALJ or the Board, as appropriate.

(b) The transcript of the testimony, exhibits, and other evidence admitted at the hearing, and all papers and requests filed in the proceeding constitute the record for decision by the ALJ and the Secretary.

(c) The record may be inspected and copied (upon payment of a reasonable fee) by any person, unless otherwise ordered by the ALJ for good cause shown.

(d) For good cause, the ALJ may order appropriate redactions made to the record.

**§ 160.544 Post hearing briefs.**

The ALJ may require the parties to file post-hearing briefs. In any event, any party may file a post-hearing brief. The ALJ must fix the time for filing the briefs. The time for filing may not exceed 60 days from the date the parties receive the transcript of the hearing or, if applicable, the stipulated record. The briefs may be accompanied by proposed findings of fact and conclusions of law. The ALJ may permit the parties to file reply briefs.

**§ 160.546 ALJ's decision.**

(a) The ALJ must issue a decision, based only on the record, which must contain findings of fact and conclusions of law.

(b) The ALJ may affirm, increase, or reduce the penalties imposed by the Secretary.

(c) The ALJ must issue the decision to both parties within 60 days after the time for submission of post-hearing briefs and reply briefs, if permitted, has expired. If the

ALJ fails to meet the deadline contained in this paragraph, he or she must notify the parties of the reason for the delay and set a new deadline.

(d) Unless the decision of the ALJ is timely appealed as provided for in § 160.548, the decision of the ALJ will be final and binding on the parties 60 days from the date of service of the ALJ's decision.

**§ 160.548 Appeal of the ALJ's decision.**

(a) Any party may appeal the decision of the ALJ to the Board by filing a notice of appeal with the Board within 30 days of the date of service of the ALJ decision. The Board may extend the initial 30 day period for a period of time not to exceed 30 days if a party files with the Board a request for an extension within the initial 30 day period and shows good cause.

(b) If a party files a timely notice of appeal with the Board, the ALJ must forward the record of the proceeding to the Board.

(c) A notice of appeal must be accompanied by a written brief specifying exceptions to the initial decision and reasons supporting the exceptions. Any party may file a brief in opposition to the exceptions, which may raise any relevant issue not addressed in the exceptions, within 30 days of receiving the notice of appeal and the accompanying brief. The Board may permit the parties to file reply briefs.

(d) There is no right to appear personally before the Board or to appeal to the Board any interlocutory ruling by the ALJ.

(e) Except for an affirmative defense under § 160.410(a)(1) or (2) of this part, the Board may not consider any issue not raised in the parties' briefs, nor any issue in the briefs that could have been raised before the ALJ but was not.

(f) If any party demonstrates to the satisfaction of the Board that additional evidence not presented at such hearing is relevant and material and that there were reasonable grounds for the failure to adduce such evidence at the hearing, the Board may remand the matter to the ALJ for consideration of such additional evidence.

(g) The Board may decline to review the case, or may affirm, increase, reduce, reverse or remand any penalty determined by the ALJ.

(h) The standard of review on a disputed issue of fact is whether the initial decision of the ALJ is supported by substantial evidence on the whole record. The standard of review on a disputed issue of law is whether the decision is erroneous.

(i) Within 60 days after the time for submission of briefs and reply briefs, if permitted, has expired, the Board must serve on each party to the appeal a copy of the Board's decision and a statement describing the right of any respondent who is penalized to seek judicial review.

(j)(1) The Board's decision under paragraph (i) of this section, including a decision to decline review of the initial decision, becomes the final decision of the Secretary 60 days after the date of service of the Board's decision, except

with respect to a decision to remand to the ALJ or if reconsideration is requested under this paragraph.

(2) The Board will reconsider its decision only if it determines that the decision contains a clear error of fact or error of law. New evidence will not be a basis for reconsideration unless the party demonstrates that the evidence is newly discovered and was not previously available.

(3) A party may file a motion for reconsideration with the Board before the date the decision becomes final under paragraph (j)(1) of this section. A motion for reconsideration must be accompanied by a written brief specifying any alleged error of fact or law and, if the party is relying on additional evidence, explaining why the evidence was not previously available. Any party may file a brief in opposition within 15 days of receiving the motion for reconsideration and the accompanying brief unless this time limit is extended by the Board for good cause shown. Reply briefs are not permitted.

(4) The Board must rule on the motion for reconsideration not later than 30 days from the date the opposition brief is due. If the Board denies the motion, the decision issued under paragraph (i) of this section becomes the final decision of the Secretary on the date of service of the ruling. If the Board grants the motion, the Board will issue a reconsidered decision, after such procedures as the Board determines necessary to address the effect of any error. The Board's decision on reconsideration becomes the final decision of the Secretary

on the date of service of the decision, except with respect to a decision to remand to the ALJ.

(5) If service of a ruling or decision issued under this section is by mail, the date of service will be deemed to be 5 days from the date of mailing.

(k)(1) A respondent's petition for judicial review must be filed within 60 days of the date on which the decision of the Board becomes the final decision of the Secretary under paragraph (j) of this section.

(2) In compliance with 28 U.S.C. 2112(a), a copy of any petition for judicial review filed in any U.S. Court of Appeals challenging the final decision of the Secretary must be sent by certified mail, return receipt requested, to the General Counsel of HHS. The petition copy must be a copy showing that it has been time-stamped by the clerk of the court when the original was filed with the court.

(3) If the General Counsel of HHS received two or more petitions within 10 days after the final decision of the Secretary, the General Counsel will notify the U.S. Judicial Panel on Multidistrict Litigation of any petitions that were received within the 10 day period.

**§ 160.550 Stay of the Secretary's decision.**

(a) Pending judicial review, the respondent may file a request for stay of the effective date of any penalty with the ALJ. The request must be accompanied by a copy of the notice of appeal filed with the Federal court. The filing of the request automatically stays the effective date of the penalty until such

time as the ALJ rules upon the request.

(b) The ALJ may not grant a respondent's request for stay of any penalty unless the respondent posts a bond or provides other adequate security.

(c) The ALJ must rule upon a respondent's request for stay within 10 days of receipt.

**§ 160.552 Harmless error.**

No error in either the admission or the exclusion of evidence, and no error or defect in any ruling or order or in any act done or omitted by the ALJ or by any of the parties is ground for vacating, modifying or otherwise disturbing an otherwise appropriate ruling or order or act, unless refusal to take such action appears to the ALJ or the Board inconsistent with substantial justice. The ALJ and the Board at every stage of the proceeding must disregard any error or defect in the proceeding that does not affect the substantial rights of the parties.

---

**PART 162—  
ADMINISTRATIVE  
REQUIREMENTS**

---

**Contents**

[Subpart A—General Provisions](#)

[§ 162.100 Applicability.](#)  
[§ 162.103 Definitions.](#)

[Subparts B-C \[Reserved\]](#)

[Subpart D—Standard Unique Health Identifier for Health Care Providers](#)

[§ 162.402 \[Reserved\]](#)  
[§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers.](#)  
[§ 162.406 Standard unique health identifier for health care providers.](#)  
[§ 162.408 National Provider System.](#)  
[§ 162.410 Implementation specifications: Health care providers.](#)  
[§ 162.412 Implementation specifications: Health plans.](#)  
[§ 162.414 Implementation specifications: Health care clearinghouses.](#)

[Subpart E—Standard Unique Health Identifier for Health Plans](#)

[§ 162.502 \[Reserved\]](#)  
[§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier.](#)  
[§ 162.506 Standard unique health plan identifier.](#)  
[§ 162.508 Enumeration System.](#)  
[§ 162.510 Full implementation requirements: Covered entities.](#)

[§ 162.512 Implementation specifications: Health plans.](#)  
[§ 162.514 Other entity identifier.](#)

[Subpart F—Standard Unique Employer Identifier](#)

[§ 162.600 Compliance dates of the implementation of the standard unique employer identifier.](#)  
[§ 162.605 Standard unique employer identifier.](#)  
[§ 162.610 Implementation specifications for covered entities.](#)

[Subparts G-H \[Reserved\]](#)

[Subpart I—General Provisions for Transactions](#)

[§ 162.900 \[Reserved\]](#)  
[§ 162.910 Maintenance of standards and adoption of modifications and new standards.](#)  
[§ 162.915 Trading partner agreements.](#)  
[§ 162.920 Availability of implementation specifications and operating rules.](#)  
[§ 162.923 Requirements for covered entities.](#)  
[§ 162.925 Additional requirements for health plans.](#)  
[§ 162.930 Additional rules for health care clearinghouses.](#)  
[§ 162.940 Exceptions from standards to permit testing of proposed modifications.](#)

[Subpart J—Code Sets](#)

[§ 162.1000 General requirements.](#)  
[§ 162.1002 Medical data code sets.](#)  
[§ 162.1011 Valid code sets.](#)

[Subpart K—Health Care Claims or Equivalent Encounter Information](#)

[§ 162.1101 Health care claims or equivalent encounter information transaction.](#)  
[§ 162.1102 Standards for health care claims or equivalent encounter information transaction.](#)

[Subpart L—Eligibility for a Health Plan](#)

[§ 162.1201 Eligibility for a health plan transaction.](#)  
[§ 162.1202 Standards for eligibility for a health plan transaction.](#)  
[§ 162.1203 Operating rules for eligibility for a health plan transaction.](#)

[Subpart M—Referral Certification and Authorization](#)

[§ 162.1301 Referral certification and authorization transaction.](#)  
[§ 162.1302 Standards for referral certification and authorization transaction.](#)

[Subpart N—Health Care Claim Status](#)

[§ 162.1401 Health care claim status transaction.](#)  
[§ 162.1402 Standards for health care claim status transaction.](#)  
[§ 162.1403 Operating rules for health care claim status transaction.](#)

[Subpart O—Enrollment and Disenrollment in a Health Plan](#)

[§ 162.1501 Enrollment and disenrollment in a health plan transaction.](#)  
[§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.](#)

[Subpart P—Health Care  
Electronic Funds Transfers  
\(EFT\) and Remittance Advice](#)

[§ 162.1601 Health care  
electronic funds transfers \(EFT\)  
and remittance advice  
transaction.](#)

[§ 162.1602 Standards for  
health care electronic funds  
transfers \(EFT\) and remittance  
advice transaction.](#)

[§ 162.1603 Operating rules for  
health care electronic funds  
transfers \(EFT\) and remittance  
advice transaction.](#)

[Subpart Q—Health Plan  
Premium Payments](#)

[§ 162.1701 Health plan  
premium payments transaction.](#)

[§ 162.1702 Standards for  
health plan premium payments  
transaction.](#)

[Subpart R—Coordination of  
Benefits](#)

[§ 162.1801 Coordination of  
benefits transaction.](#)

[§ 162.1802 Standards for  
coordination of benefits  
information transaction.](#)

[Subpart S—Medicaid Pharmacy  
Subrogation](#)

[§ 162.1901 Medicaid  
pharmacy subrogation  
transaction.](#)

[§ 162.1902 Standard for  
Medicaid pharmacy subrogation  
transaction.](#)

---

AUTHORITY: Secs. 1171 through 1180 of the Social Security Act (42 U.S.C. 1320d-1320d-9), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, sec. 105 of Pub. L. 110-233, 122 Stat. 881-922, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-

2034 (42 U.S.C. 1320d-2(note), and secs. 1104 and 10109 of Pub. L. 111-148, 124 Stat. 146-154 and 915-917.

SOURCE: 65 FR 50367, Aug. 17, 2000, unless otherwise noted.

**Subpart A—General Provisions**

**§ 162.100 Applicability.**

Covered entities (as defined in § 160.103 of this subchapter) must comply with the applicable requirements of this part.

**§ 162.103 Definitions.**

For purposes of this part, the following definitions apply:

*Code set* means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

*Code set maintaining organization* means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part.

*Controlling health plan (CHP)* means a health plan that—

(1) Controls its own business activities, actions, or policies; or

(2)(i) Is controlled by an entity that is not a health plan; and

(ii) If it has a subhealth plan(s) (as defined in this section), exercises sufficient control over the subhealth plan(s) to direct

its/their business activities, actions, or policies.

*Covered health care provider* means a health care provider that meets the definition at paragraph (3) of the definition of “covered entity” at § 160.103.

*Data condition* means the rule that describes the circumstances under which a covered entity must use a particular data element or segment.

*Data content* means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not data content.

*Data element* means the smallest named unit of information in a transaction.

*Data set* means a semantically meaningful unit of information exchanged between two parties to a transaction.

*Descriptor* means the text defining a code.

*Designated standard maintenance organization (DSMO)* means an organization designated by the Secretary under § 162.910(a).

*Direct data entry* means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer.

*Format* refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction.

*HCPCS* stands for the Health [Care Financing Administration] Common Procedure Coding System.

*Maintain* or *maintenance* refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification.

*Maximum defined data set* means all of the required data elements for a particular standard based on a specific implementation specification.

*Operating rules* means the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications as adopted for purposes of this part.

*Segment* means a group of related data elements in a transaction.

*Stage 1 payment initiation* means a health plan's order, instruction or authorization to its financial institution to make a health care claims payment using an electronic funds transfer (EFT) through the ACH Network.

*Standard transaction* means a transaction that complies with an applicable standard and associated operating rules adopted under this part.

*Subhealth plan (SHP)* means a health plan whose business activities, actions, or policies are directed by a controlling health plan.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8374, Feb. 20, 2003; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 77 FR 54719, Sept. 5, 2012]

#### **Subparts B-C [Reserved]**

#### **Subpart D—Standard Unique Health Identifier for Health Care Providers**

SOURCE: 69 FR 3468, Jan. 23, 2004, unless otherwise noted.

#### **§ 162.402 [Reserved]**

#### **§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers.**

(a) *Health care providers.* A covered health care provider must comply with the implementation specifications in § 162.410 no later than May 23, 2007.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.412 no later than one of the following dates:

(1) A health plan that is not a small health plan—May 23, 2007.

(2) A small health plan—May 23, 2008.

(c) *Health care clearinghouses.* A health care clearinghouse

must comply with the implementation specifications in § 162.414 no later than May 23, 2007.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

#### **§ 162.406 Standard unique health identifier for health care providers.**

(a) *Standard.* The standard unique health identifier for health care providers is the National Provider Identifier (NPI). The NPI is a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number.

(b) *Required and permitted uses for the NPI.* (1) The NPI must be used as stated in § 162.410, § 162.412, and § 162.414.

(2) The NPI may be used for any other lawful purpose.

#### **§ 162.408 National Provider System.**

*National Provider System.* The National Provider System (NPS) shall do the following:

(a) Assign a single, unique NPI to a health care provider, provided that—

(1) The NPS may assign an NPI to a subpart of a health care provider in accordance with paragraph (g); and

(2) The Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health

care provider that has been assigned an NPI and perform tasks necessary to update that information.

(c) If appropriate, deactivate an NPI upon receipt of appropriate information concerning the dissolution of the health care provider that is an organization, the death of the health care provider who is an individual, or other circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated NPI upon receipt of appropriate information.

(e) Not assign a deactivated NPI to any other health care provider.

(f) Disseminate NPS information upon approved requests.

(g) Assign an NPI to a subpart of a health care provider on request if the identifying data for the subpart are unique.

**§ 162.410 Implementation specifications: Health care providers.**

(a) A covered entity that is a covered health care provider must:

(1) Obtain, by application if necessary, an NPI from the National Provider System (NPS) for itself or for any subpart of the covered entity that would be a covered health care provider if it were a separate legal entity. A covered entity may obtain an NPI for any other subpart that qualifies for the assignment of an NPI.

(2) Use the NPI it obtained from the NPS to identify itself on all

standard transactions that it conducts where its health care provider identifier is required.

(3) Disclose its NPI, when requested, to any entity that needs the NPI to identify that covered health care provider in a standard transaction.

(4) Communicate to the NPS any changes in its required data elements in the NPS within 30 days of the change.

(5) If it uses one or more business associates to conduct standard transactions on its behalf, require its business associate(s) to use its NPI and other NPIs appropriately as required by the transactions that the business associate(s) conducts on its behalf.

(6) If it has been assigned NPIs for one or more subparts, comply with the requirements of paragraphs (a)(2) through (a)(5) of this section with respect to each of those NPIs.

(b) An organization covered health care provider that has as a member, employs, or contracts with, an individual health care provider who is not a covered entity and is a prescriber, must require such health care provider to—

(1) Obtain an NPI from the National Plan and Provider Enumeration System (NPPES); and

(2) To the extent the prescriber writes a prescription while acting within the scope of the prescriber's relationship with the organization, disclose the NPI upon request to any entity that needs it to identify the prescriber in a standard transaction.

(c) A health care provider that is not a covered entity may obtain, by application if necessary, an NPI from the NPS.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

**§ 162.412 Implementation specifications: Health plans.**

(a) A health plan must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

(b) A health plan may not require a health care provider that has been assigned an NPI to obtain an additional NPI.

**§ 162.414 Implementation specifications: Health care clearinghouses.**

A health care clearinghouse must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

**Subpart E—Standard Unique Health Identifier for Health Plans**

SOURCE: 77 FR 54719, Sept. 5, 2012, unless otherwise noted.

**§ 162.502 [Reserved]**

**§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier.**

(a) *Covered entities.* A covered entity must comply with the implementation requirements in § 162.510 no later than November 7, 2016.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.512 no later than one of the following dates:

(1) A health plan that is not a small health plan— November 5, 2014.

(2) A health plan that is a small health plan— November 5, 2015.

[77 FR 54719, Sept. 5, 2012, as amended at 77 FR 60630, Oct. 4, 2012]

#### **§ 162.506 Standard unique health plan identifier.**

(a) *Standard.* The standard unique health plan identifier is the Health Plan Identifier (HPID) that is assigned by the Enumeration System identified in § 162.508.

(b) *Required and permitted uses for the HPID.* (1) The HPID must be used as specified in § 162.510 and § 162.512.

(2) The HPID may be used for any other lawful purpose.

#### **§ 162.508 Enumeration System.**

The Enumeration System must do all of the following:

(a) Assign a single, unique—

(1) HPID to a health plan, provided that the Secretary has

sufficient information to permit the assignment to be made; or

(2) OEID to an entity eligible to receive one under § 162.514(a), provided that the Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health plan that applies for or has been assigned an HPID and each entity that applies for or has been assigned an OEID, and perform tasks necessary to update that information.

(c) If appropriate, deactivate an HPID or OEID upon receipt of sufficient information concerning circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated HPID or OEID upon receipt of sufficient information justifying reactivation.

(e) Not assign a deactivated HPID to any other health plan or OEID to any other entity.

(f) Disseminate Enumeration System information upon approved requests.

#### **§ 162.510 Full implementation requirements: Covered entities.**

(a) A covered entity must use an HPID to identify a health plan that has an HPID when a covered entity identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

(b) If a covered entity uses one or more business associates to conduct standard transactions on its behalf, it must require its business associate(s) to use an

HPID to identify a health plan that has an HPID when the business associate(s) identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

#### **§ 162.512 Implementation specifications: Health plans.**

(a) A controlling health plan must do all of the following:

(1) Obtain an HPID from the Enumeration System for itself.

(2) Disclose its HPID, when requested, to any entity that needs the HPID to identify the health plan in a standard transaction.

(3) Communicate to the Enumeration System any changes in its required data elements in the Enumeration System within 30 days of the change.

(b) A controlling health plan may do the following:

(1) Obtain an HPID from the Enumeration System for a subhealth plan of the controlling health plan.

(2) Direct a subhealth plan of the controlling health plan to obtain an HPID from the Enumeration System.

(c) A subhealth plan may obtain an HPID from the Enumeration System.

(d) A subhealth plan that is assigned an HPID from the Enumeration System must comply with the requirements that apply to a controlling health plan in paragraphs (a)(2) and (a)(3) of this section.



**§ 162.514 Other entity identifier.**

(a) An entity may obtain an Other Entity Identifier (OEID) to identify itself if the entity meets all of the following:

(1) Needs to be identified in a transaction for which the Secretary has adopted a standard under this part.

(2) Is not eligible to obtain an HPID.

(3) Is not eligible to obtain an NPI.

(4) Is not an individual.

(b) An OEID must be obtained from the Enumeration System identified in § 162.508.

(c) *Uses for the OEID.* (1) An other entity may use the OEID it obtained from the Enumeration System to identify itself or have itself identified on all covered transactions in which it needs to be identified.

(2) The OEID may be used for any other lawful purpose.

**Subpart F—Standard Unique Employer Identifier**

SOURCE: 67 FR 38020, May 31, 2002, unless otherwise noted.

**§ 162.600 Compliance dates of the implementation of the standard unique employer identifier.**

(a) *Health care providers.* Health care providers must comply with the requirements of this subpart no later than July 30, 2004.

(b) *Health plans.* A health plan must comply with the requirements of this subpart no later than one of the following dates:

(1) *Health plans other than small health plans* —July 30, 2004.

(2) *Small health plans* —August 1, 2005.

(c) *Health care clearinghouses.* Health care clearinghouses must comply with the requirements of this subpart no later than July 30, 2004.

**§ 162.605 Standard unique employer identifier.**

The Secretary adopts the EIN as the standard unique employer identifier provided for by 42 U.S.C. 1320d-2(b).

**§ 162.610 Implementation specifications for covered entities.**

(a) The standard unique employer identifier of an employer of a particular employee is the EIN that appears on that employee's IRS Form W-2, Wage and Tax Statement, from the employer.

(b) A covered entity must use the standard unique employer identifier (EIN) of the appropriate employer in standard transactions that require an employer identifier to identify a person or entity as an employer, including where situationally required.

(c) Required and permitted uses for the Employer Identifier.

(1) The Employer Identifier must be used as stated in § 162.610(b).

(2) The Employer Identifier may be used for any other lawful purpose.

[67 FR 38020, May 31, 2002, as amended at 69 FR 3469, Jan. 23, 2004]

**Subparts G-H [Reserved]**

**Subpart I—General Provisions for Transactions**

**§ 162.900 [Reserved]**

**§ 162.910 Maintenance of standards and adoption of modifications and new standards.**

(a) *Designation of DSMOs.* (1) The Secretary may designate as a DSMO an organization that agrees to conduct, to the satisfaction of the Secretary, the following functions:

(i) Maintain standards adopted under this subchapter.

(ii) Receive and process requests for adopting a new standard or modifying an adopted standard.

(2) The Secretary designates a DSMO by notice in the FEDERAL REGISTER.

(b) *Maintenance of standards.* Maintenance of a standard by the appropriate DSMO constitutes maintenance of the standard for purposes of this part, if done in accordance with the processes the Secretary may require.

(c) *Process for modification of existing standards and adoption*

*of new standards.* The Secretary considers a recommendation for a proposed modification to an existing standard, or a proposed new standard, only if the recommendation is developed through a process that provides for the following:

- (1) Open public access.
- (2) Coordination with other DSMOs.
- (3) An appeals process for each of the following, if dissatisfied with the decision on the request:
  - (i) The requestor of the proposed modification.
  - (ii) A DSMO that participated in the review and analysis of the request for the proposed modification, or the proposed new standard.
- (4) Expedited process to address content needs identified within the industry, if appropriate.
- (5) Submission of the recommendation to the National Committee on Vital and Health Statistics (NCVHS).

**§ 162.915 Trading partner agreements.**

A covered entity must not enter into a trading partner agreement that would do any of the following:

- (a) Change the definition, data condition, or use of a data element or segment in a standard or operating rule, except where necessary to implement State or Federal law, or to protect against fraud and abuse.

(b) Add any data elements or segments to the maximum defined data set.

(c) Use any code or data elements that are either marked “not used” in the standard's implementation specification or are not in the standard's implementation specification(s).

(d) Change the meaning or intent of the standard's implementation specification(s).

[65 FR 50367, Aug. 17, 2000, as amended at 76 FR 40495, July 8, 2011]

**§ 162.920 Availability of implementation specifications and operating rules.**

Certain material is incorporated by reference into this subpart with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, the Department of Health and Human Services must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. All approved material is available for inspection at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call (202) 714-6030, or go to: [http://www.archives.gov/federal\\_register/code\\_of\\_federal\\_regulations/ibr\\_locations.html](http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html). The materials are also available for inspection by the public at the Centers for Medicare & Medicaid Services (CMS), 7500 Security Boulevard, Baltimore, Maryland 21244. For more information on the availability on the materials at CMS, call (410) 786-6597. The materials

are also available from the sources listed below.

(a) *ASC X12N specifications and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3.* The implementation specifications for the ASC X12N and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 (and accompanying Errata or Type 1 Errata) may be obtained from the ASC X12, 7600 Leesburg Pike, Suite 430, Falls Church, VA 22043; Telephone (703) 970-4480; and FAX (703) 970-4488. They are also available through the internet at <http://www.X12.org>. A fee is charged for all implementation specifications, including Technical Reports Type 3. Charging for such publications is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1, as referenced in § 162.1102 and § 162.1802.

(2) The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1, as referenced in § 162.1102 and § 162.1802.

(3) The ASC X12N 837—  
Health Care Claim: Institutional,  
Volumes 1 and 2, Version 4010,  
May 2000, Washington  
Publishing Company,  
004010X096 and Addenda to  
Health Care Claim: Institutional,  
Volumes 1 and 2, Version 4010,  
October 2002, Washington  
Publishing Company,  
004010X096A1 as referenced in  
§ 162.1102 and § 162.1802.

(4) The ASC X12N 835—  
Health Care Claim  
Payment/Advice, Version 4010,  
May 2000, Washington  
Publishing Company,  
004010X091, and Addenda to  
Health Care Claim  
Payment/Advice, Version 4010,  
October 2002, Washington  
Publishing Company,  
004010X091A1 as referenced in  
§ 162.1602.

(5) ASC X12N 834—Benefit  
Enrollment and Maintenance,  
Version 4010, May 2000,  
Washington Publishing  
Company, 004010X095 and  
Addenda to Benefit Enrollment  
and Maintenance, Version 4010,  
October 2002, Washington  
Publishing Company,  
004010X095A1, as referenced  
in § 162.1502.

(6) The ASC X12N 820—  
Payroll Deducted and Other  
Group Premium Payment for  
Insurance Products, Version  
4010, May 2000, Washington  
Publishing Company,  
004010X061, and Addenda to  
Payroll Deducted and Other  
Group Premium Payment for  
Insurance Products, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X061A1, as  
referenced in § 162.1702.

(7) The ASC X12N 278—  
Health Care Services Review—

Request for Review and  
Response, Version 4010, May  
2000, Washington Publishing  
Company, 004010X094 and  
Addenda to Health Care  
Services Review—Request for  
Review and Response, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X094A1, as  
referenced in § 162.1302.

(8) The ASC X12N-276/277  
Health Care Claim Status  
Request and Response, Version  
4010, May 2000, Washington  
Publishing Company,  
004010X093 and Addenda to  
Health Care Claim Status  
Request and Response, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X093A1, as  
referenced in § 162.1402.

(9) The ASC X12N 270/271—  
Health Care Eligibility Benefit  
Inquiry and Response, Version  
4010, May 2000, Washington  
Publishing Company,  
004010X092 and Addenda to  
Health Care Eligibility Benefit  
Inquiry and Response, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X092A1, as  
referenced in § 162.1202.

(10) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Health Care Claim: Dental  
(837), May 2006, ASC  
X12N/005010X224, and Type 1  
Errata to Health Care Claim  
Dental (837), ASC X12  
Standards for Electronic Data  
Interchange Technical Report  
Type 3, October 2007, ASC  
X12N/005010X224A1, as  
referenced in § 162.1102 and  
§ 162.1802.

(11) The ASC X12 Standards  
for Electronic Data Interchange

Technical Report Type 3—  
Health Care Claim: Professional  
(837), May 2006, ASC X12,  
005010X222, as referenced in  
§ 162.1102 and § 162.1802.

(12) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Health Care Claim: Institutional  
(837), May 2006, ASC  
X12/N005010X223, and Type 1  
Errata to Health Care Claim:  
Institutional (837), ASC X12  
Standards for Electronic Data  
Interchange Technical Report  
Type 3, October 2007, ASC  
X12N/005010X223A1, as  
referenced in § 162.1102 and  
§ 162.1802.

(13) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Health Care Claim  
Payment/Advice (835), April  
2006, ASC X12N/005010X221,  
as referenced in § 162.1602.

(14) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Benefit Enrollment and  
Maintenance (834), August  
2006, ASC X12N/005010X220,  
as referenced in § 162.1502.

(15) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Payroll Deducted and Other  
Group Premium Payment for  
Insurance Products (820),  
February 2007, ASC  
X12N/005010X218, as  
referenced in § 162.1702.

(16) The ASC X12 Standards  
for Electronic Data Interchange  
Technical Report Type 3—  
Health Care Services Review—  
Request for Review and  
Response (278), May 2006,  
ASC X12N/005010X217, and  
Errata to Health Care Services

Review—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1, as referenced in § 162.1302.

(17) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1, as referenced in § 162.1402.

(18) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279, as referenced in § 162.1202.

(b) *Retail pharmacy specifications and Medicaid subrogation implementation guides.* The implementation specifications for the retail pharmacy standards and the implementation specifications for the batch standard for the Medicaid pharmacy subrogation transaction may be obtained from the National Council for Prescription Drug Programs, 9240 East Raintree Drive, Scottsdale, AZ 85260. Telephone (480) 477-1000; FAX (480) 767-1042. They are also available through the Internet at <http://www.ncdp.org>. A fee is charged for all NCPDP Implementation Guides. Charging for such publications

is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The Telecommunication Standard Implementation Guide Version 5, Release 1 (Version 5.1), September 1999, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, § 162.1602, and § 162.1802.

(2) The Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(3) The National Council for Prescription Drug Programs (NCPDP) equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 0, February 1, 1996, as referenced in § 162.1102, § 162.1202, § 162.1602, and § 162.1802.

(4) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(5) The Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), January 2006, National Council for Prescription Drug Programs, as referenced in § 162.1102,

§ 162.1202, § 162.1302, and § 162.1802.

(6) The Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902.

(c) Council for Affordable Quality Healthcare's (CAQH) Committee on Operating Rules for Information Exchange (CORE), 601 Pennsylvania Avenue, NW. South Building, Suite 500 Washington, DC 20004; Telephone (202) 861-1492; Fax (202) 861-1454; E-mail [info@CAQH.org](mailto:info@CAQH.org); and Internet at <http://www.caqh.org/benefits.php>.

(1) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase I Policies and Operating Rules, Approved April 2006, v5010 Update March 2011.

(i) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(ii) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase I CORE 155: Eligibility and Benefits Batch Response Time Rule, version

1.1.0, March 2011, as referenced in § 162.1203.

(v) Phase I CORE 156: Eligibility and Benefits Real Time Response Time Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(vi) Phase I CORE 157: Eligibility and Benefits System Availability Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(2) ACME Health Plan, HIPAA Transaction Standard Companion Guide, Refers to the Implementation Guides Based on ASC X12 version 005010, CORE v5010 Master Companion Guide Template, 005010, 1.2, (CORE v 5010 Master Companion Guide Template, 005010, 1.2), March 2011, as referenced in §§ 162.1203, 162.1403, and 162.1603.

(3) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase II Policies and Operating Rules, Approved July 2008, v5010 Update March 2011.

(i) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, as referenced in § 162.1403.

(ii) Phase II CORE 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase II CORE 259: Eligibility and Benefits 270/271 AAA Error Code Reporting Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase II CORE 260: Eligibility & Benefits Data Content (270/271) Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(v) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011, as referenced in § 162.1203 and § 162.1403.

(4) Council for Affordable Quality Healthcare (CAQH) Phase III Committee on Operating Rules for Information Exchange (CORE) EFT & ERA Operating Rule Set, Approved June 2012, as specified in this paragraph and referenced in § 162.1603.

(i) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(ii) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(iii) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(iv) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(v) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(vi) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled “Health Care Claim Payment/Advice

Batch Acknowledgement Requirements”.

(d) The National Automated Clearing House Association (NACHA), The Electronic Payments Association, 1350 Sunrise Valle Drive, Suite 100, Herndon, Virginia 20171 (Phone) (703) 561-1100; (Fax) (703) 713-1641; Email: [info@nacha.org](mailto:info@nacha.org); and Internet at <http://www.nacha.org>. The implementation specifications are as follows:

(1) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules, Appendix One: ACH File Exchange Specifications (Operating Rule 59) as referenced in § 162.1602.

(2) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules Appendix Three: ACH Record Format Specifications (Operating Rule 78), Part 3.1, Subpart 3.1.8 Sequence of Records for CCD Entries as referenced in § 162.1602.

[68 FR 8396, Feb. 20, 2003, as amended at 69 FR 18803, Apr. 9, 2004; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

### **§ 162.923 Requirements for covered entities.**

(a) *General rule.* Except as otherwise provided in this part, if a covered entity conducts, with another covered entity that is required to comply with a transaction standard adopted

under this part (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard under this part, the covered entity must conduct the transaction as a standard transaction.

(b) *Exception for direct data entry transactions.* A health care provider electing to use direct data entry offered by a health plan to conduct a transaction for which a standard has been adopted under this part must use the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard.

(c) *Use of a business associate.* A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:

- (1) Comply with all applicable requirements of this part.
- (2) Require any agent or subcontractor to comply with all applicable requirements of this part.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

**§ 162.925 Additional requirements for health plans.**

(a) *General rules.* (1) If an entity requests a health plan to conduct

a transaction as a standard transaction, the health plan must do so.

(2) A health plan may not delay or reject a transaction, or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction.

(3) A health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).

(4) A health plan may not offer an incentive for a health care provider to conduct a transaction covered by this part as a transaction described under the exception provided for in § 162.923(b).

(5) A health plan that operates as a health care clearinghouse, or requires an entity to use a health care clearinghouse to receive, process, or transmit a standard transaction may not charge fees or costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard transaction to, or from, a health plan.

(6) During the period from March 17, 2009 through December 31, 2011, a health plan may not delay or reject a standard transaction, or attempt to adversely affect the other entity or the transaction, on the basis that it does not comply with another adopted standard for the same period.

(b) *Coordination of benefits.* If a health plan receives a standard transaction and coordinates

benefits with another health plan (or another payer), it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan (or other payer).

(c) *Code sets.* A health plan must meet each of the following requirements:

(1) Accept and promptly process any standard transaction that contains codes that are valid, as provided in subpart J of this part.

(2) Keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

**§ 162.930 Additional rules for health care clearinghouses.**

When acting as a business associate for another covered entity, a health care clearinghouse may perform the following functions:

(a) Receive a standard transaction on behalf of the covered entity and translate it into a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) for transmission to the covered entity.

(b) Receive a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) from the covered entity and translate it into a standard transaction for transmission on behalf of the covered entity.

**§ 162.940 Exceptions from standards to permit testing of proposed modifications.**

*(a) Requests for an exception.*

An organization may request an exception from the use of a standard from the Secretary to test a proposed modification to that standard. For each proposed modification, the organization must meet the following requirements:

(1) *Comparison to a current standard.* Provide a detailed explanation, no more than 10 pages in length, of how the proposed modification would be a significant improvement to the current standard in terms of the following principles:

(i) Improve the efficiency and effectiveness of the health care system by leading to cost reductions for, or improvements in benefits from, electronic health care transactions.

(ii) Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses.

(iii) Be uniform and consistent with the other standards adopted under this part and, as appropriate, with other private and public sector health data standards.

(iv) Have low additional development and implementation costs relative to the benefits of using the standard.

(v) Be supported by an ANSI-accredited SSO or other private or public organization that would maintain the standard over time.

(vi) Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster.

(vii) Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, unless they are explicitly part of the standard.

(viii) Be precise, unambiguous, and as simple as possible.

(ix) Result in minimum data collection and paperwork burdens on users.

(x) Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology.

(2) *Specifications for the proposed modification.* Provide specifications for the proposed modification, including any additional system requirements.

(3) *Testing of the proposed modification.* Provide an explanation, no more than 5 pages in length, of how the organization intends to test the standard, including the number and types of health plans and health care providers expected to be involved in the test, geographical areas, and beginning and ending dates of the test.

(4) *Trading partner concurrences.* Provide written concurrences from trading partners who would agree to participate in the test.

(b) *Basis for granting an exception.* The Secretary may grant an initial exception, for a period not to exceed 3 years, based on, but not limited to, the following criteria:

(1) An assessment of whether the proposed modification demonstrates a significant improvement to the current standard.

(2) The extent and length of time of the exception.

(3) Consultations with DSMOs.

(c) *Secretary's decision on exception.* The Secretary makes a decision and notifies the organization requesting the exception whether the request is granted or denied.

(1) *Exception granted.* If the Secretary grants an exception, the notification includes the following information:

(i) The length of time for which the exception applies.

(ii) The trading partners and geographical areas the Secretary approves for testing.

(iii) Any other conditions for approving the exception.

(2) *Exception denied.* If the Secretary does not grant an exception, the notification explains the reasons the Secretary considers the proposed modification would not be a significant improvement to the current standard and any other rationale for the denial.

(d) *Organization's report on test results.* Within 90 days after the test is completed, an organization that receives an

exception must submit a report on the results of the test, including a cost-benefit analysis, to a location specified by the Secretary by notice in the FEDERAL REGISTER.

(e) *Extension allowed.* If the report submitted in accordance with paragraph (d) of this section recommends a modification to the standard, the Secretary, on request, may grant an extension to the period granted for the exception.

## Subpart J—Code Sets

### § 162.1000 General requirements.

When conducting a transaction covered by this part, a covered entity must meet the following requirements:

(a) *Medical data code sets.* Use the applicable medical data code sets described in § 162.1002 as specified in the implementation specification adopted under this part that are valid at the time the health care is furnished.

(b) *Nonmedical data code sets.* Use the nonmedical data code sets as described in the implementation specifications adopted under this part that are valid at the time the transaction is initiated.

### § 162.1002 Medical data code sets.

The Secretary adopts the following maintaining organization's code sets as the standard medical data code sets:

(a) For the period from October 16, 2002 through October 15, 2003:

(1) *International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

- (i) Diseases.
- (ii) Injuries.
- (iii) Impairments.
- (iv) Other health problems and their manifestations.
- (v) Causes of injury, disease, impairment, or other health problems.

(2) *International Classification of Diseases, 9th Edition, Clinical Modification, Volume 3 Procedures* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

- (i) Prevention.
- (ii) Diagnosis.
- (iii) Treatment.
- (iv) Management.

(3) *National Drug Codes (NDC)*, as maintained and distributed by HHS, in collaboration with drug manufacturers, for the following:

- (i) Drugs

(ii) Biologics.

(4) *Code on Dental Procedures and Nomenclature*, as maintained and distributed by the American Dental Association, for dental services.

(5) The combination of *Health Care Financing Administration Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, and *Current Procedural Terminology, Fourth Edition (CPT-4)*, as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following:

- (i) Physician services.
- (ii) Physical and occupational therapy services.
- (iii) Radiologic procedures.
- (iv) Clinical laboratory tests.
- (v) Other medical diagnostic procedures.
- (vi) Hearing and vision services.
- (vii) Transportation services including ambulance.

(6) The *Health Care Financing Administration Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services. These items include, but are not limited to, the following:

- (i) Medical supplies.



(ii) Orthotic and prosthetic devices.

(iii) Durable medical equipment.

(b) For the period on and after October 16, 2003 through September 30, 2014:

(1) The code sets specified in paragraphs (a)(1), (a)(2),(a)(4), and (a)(5) of this section.

(2) *National Drug Codes (NDC)*, as maintained and distributed by HHS, for reporting the following by retail pharmacies:

(i) Drugs.

(ii) Biologics.

(3) *The Healthcare Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services, with the exception of drugs and biologics. These items include, but are not limited to, the following:

(i) Medical supplies.

(ii) Orthotic and prosthetic devices.

(iii) Durable medical equipment.

(c) For the period on and after October 1, 2014:

(1) The code sets specified in paragraphs (a)(4), (a)(5), (b)(2), and (b)(3) of this section.

(2) International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM) (including The Official ICD-10-CM Guidelines for

Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

(i) Diseases.

(ii) Injuries.

(iii) Impairments.

(iv) Other health problems and their manifestations.

(v) Causes of injury, disease, impairment, or other health problems.

(3) International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) (including The Official ICD-10-PCS Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

(i) Prevention.

(ii) Diagnosis.

(iii) Treatment.

(iv) Management.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8397, Feb. 20, 2003; 74 FR 3362, Jan. 16, 2009; 77 FR 54720, Sept. 5, 2012]

**§ 162.1011 Valid code sets.**

Each code set is valid within the dates specified by the organization responsible for maintaining that code set.

**Subpart K—Health Care Claims or Equivalent Encounter Information**

**§ 162.1101 Health care claims or equivalent encounter information transaction.**

The health care claims or equivalent encounter information transaction is the transmission of either of the following:

(a) A request to obtain payment, and the necessary accompanying information from a health care provider to a health plan, for health care.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

**§ 162.1102 Standards for health care claims or equivalent encounter information transaction.**

The Secretary adopts the following standards for the health care claims or equivalent encounter information transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs claims.* The National Council for Prescription Drug Programs (NCPDP) Telecommunication Standards Implementation Guide, Version 5, Release 1, September 1999, and equivalent NCPDP Batch Standards Batch Implementation Guide, Version

1, Release 1, (Version 1.1), January 2000, supporting Telecommunication Version 5.1 for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, health care claims.* The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097. and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims.* The ASC X12N 837—Health Care Claims: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claims: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010x098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims.* The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1)(i) The standards identified in paragraph (a) of this section; and

(ii) For retail pharmacy supplies and professional services claims, the following: The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096, October 2002 (Incorporated by reference in § 162.920); and

(2)(i) *Retail pharmacy drug claims.* The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007 and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837) ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) *Professional health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(iv) *Institutional health care claims.* The ASC X12 Standards

for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837) ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(v) *Retail pharmacy supplies and professional services claims.* (A) The Telecommunication Standard, Implementation Guide Version 5, Release 1, September 1999. (Incorporated by reference in § 162.920.)

(B) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs (Incorporated by reference in § 162.920); and

(C) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(c) For the period on and after the January 1, 2012, the standards identified in paragraph (b)(2) of this section, except the standard identified in paragraph (b)(2)(v)(A) of this section.

[68 FR 8397, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3325, Jan. 16, 2009]

**Subpart L—Eligibility for a Health Plan**

**§ 162.1201 Eligibility for a health plan transaction.**

The eligibility for a health plan transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

(1) Eligibility to receive health care under the health plan.

(2) Coverage of health care under the health plan.

(3) Benefits associated with the benefit plan.

(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.

**§ 162.1202 Standards for eligibility for a health plan transaction.**

The Secretary adopts the following standards for the eligibility for a health plan transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs*. The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch

Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000 supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, professional, and institutional health care eligibility benefit inquiry and response*. The ASC X12N 270/271—Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, Washington Publishing Company, 004010X092A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011 both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs*. The Telecommunication Standard Implementation Guide Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental, professional, and institutional health care eligibility benefit inquiry and response*. The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility

Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

**§ 162.1203 Operating rules for eligibility for a health plan transaction.**

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase I and Phase II operating rules (updated for Version 5010) for the eligibility for a health plan transaction:

(1) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, and CORE v5010 Master Companion Guide Template. (Incorporated by reference in § 162.920).

(2) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(3) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(4) Phase I CORE 155:  
Eligibility and Benefits Batch  
Response Time Rule, version  
1.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(5) Phase I CORE 156:  
Eligibility and Benefits Real  
Time Response Rule, version  
1.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(6) Phase I CORE 157:  
Eligibility and Benefits System  
Availability Rule, version 1.1.0,  
March 2011. (Incorporated by  
reference in § 162.920).

(7) Phase II CORE 258:  
Eligibility and Benefits 270/271  
Normalizing Patient Last Name  
Rule, version 2.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(8) Phase II CORE 259:  
Eligibility and Benefits 270/271  
AAA Error Code Reporting  
Rule, version 2.1.0.  
(Incorporated by reference in  
§ 162.920).

(9) Phase II CORE 260:  
Eligibility & Benefits Data  
Content (270/271) Rule, version  
2.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(10) Phase II CORE 270:  
Connectivity Rule, version  
2.2.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(b) Excluding where the CAQH  
CORE rules reference and  
pertain to acknowledgements  
and CORE certification.

[76 FR 40496, July 8, 2011]

### **Subpart M—Referral Certification and Authorization**

#### **§ 162.1301 Referral certification and authorization transaction.**

The referral certification and  
authorization transaction is any  
of the following transmissions:

(a) A request from a health care  
provider to a health plan for the  
review of health care to obtain  
an authorization for the health  
care.

(b) A request from a health care  
provider to a health plan to  
obtain authorization for referring  
an individual to another health  
care provider.

(c) A response from a health  
plan to a health care provider to  
a request described in paragraph  
(a) or paragraph (b) of this  
section.

[74 FR 3326, Jan. 16, 2009]

#### **§ 162.1302 Standards for referral certification and authorization transaction.**

The Secretary adopts the  
following standards for the  
referral certification and  
authorization transaction:

(a) For the period from October  
16, 2003 through March 16,  
2009:

(1) *Retail pharmacy drug  
referral certification and  
authorization.* The NCPDP  
Telecommunication Standard  
Implementation Guide, Version  
5, Release 1 (Version 5.1),  
September 1999, and equivalent  
NCPDP Batch Standard Batch  
Implementation Guide, Version

1, Release 1 (Version 1.1),  
January 2000, supporting  
Telecommunications Standard  
Implementation Guide, Version  
5, Release 1 (Version 5.1) for  
the NCPDP Data Record in the  
Detail Data Record.  
(Incorporated by reference in  
§ 162.920).

(2) *Dental, professional, and  
institutional referral  
certification and authorization.*  
The ASC X12N 278—Health  
Care Services Review—Request  
for Review and Response,  
Version 4010, May 2000,  
Washington Publishing  
Company, 004010X094 and  
Addenda to Health Care  
Services Review—Request for  
Review and Response, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X094A1.  
(Incorporated by reference in  
§ 162.920).

(b) For the period from March  
17, 2009 through December 31,  
2011 both—

(1) The standards identified in  
paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs.*  
The Telecommunication  
Standard Implementation Guide  
Version D, Release 0 (Version  
D.0), August 2007, and  
equivalent Batch Standard  
Implementation Guide, Version  
1, Release 2 (Version 1.2),  
National Council for  
Prescription Drug Programs.  
(Incorporated by reference in  
§ 162.920.)

(ii) *Dental, professional, and  
institutional request for review  
and response.* The ASC X12  
Standards for Electronic Data  
Interchange Technical Report  
Type 3—Health Care Services  
Review—Request for Review

and Response (278), May 2006, ASC X12N/005010X217, and Errata to Health Care Services Review—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

#### **Subpart N—Health Care Claim Status**

##### **§ 162.1401 Health care claim status transaction.**

The health care claim status transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan to determine the status of a health care claim.

(b) A response from a health plan to a health care provider about the status of a health care claim.

[74 FR 3326, Jan. 16, 2009]

##### **§ 162.1402 Standards for health care claim status transaction.**

The Secretary adopts the following standards for the health care claim status transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N-276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 and Addenda to Health Care Claim Status Request and Response, Version 4010, October 2002, Washington Publishing Company, 004010X093A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3326, Jan. 16, 2009]

##### **§ 162.1403 Operating rules for health care claim status transaction.**

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase II operating rules (updated for Version 5010) for the health care claim status transaction:

(1) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, and CORE v5010 Master Companion Guide, 00510, 1.2, March 2011. (Incorporated by reference in § 162.920).

(2) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011. (Incorporated by reference in § 162.920).

(b) Excluding where the CAQH CORE rules reference and pertain to acknowledgements and CORE certification.

[76 FR 40496, July 8, 2011]

#### **Subpart O—Enrollment and Disenrollment in a Health Plan**

##### **§ 162.1501 Enrollment and disenrollment in a health plan transaction.**

The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information from the sponsor of the insurance coverage, benefits, or policy, to a health plan to establish or terminate insurance coverage.

[74 FR 3327, Jan. 16, 2009]

##### **§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.**

The Secretary adopts the following standards for

enrollment and disenrollment in a health plan transaction.

(a) For the period from October 16, 2003 through March 16, 2009: ASC X12N 834—Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 and Addenda to Benefit Enrollment and Maintenance, Version 4010, October 2002, Washington Publishing Company, 004010X095A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220 (Incorporated by reference in § 162.920)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

#### **Subpart P—Health Care Electronic Funds Transfers (EFT) and Remittance Advice**

#### **§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction.**

The health care electronic funds transfers (EFT) and remittance advice transaction is the transmission of either of the following for health care:

(a) The transmission of any of the following from a health plan to a health care provider:

- (1) Payment.
- (2) Information about the transfer of funds.
- (3) Payment processing information.

(b) The transmission of either of the following from a health plan to a health care provider:

- (1) Explanation of benefits.
- (2) Remittance advice.

[65 FR 50367, Aug. 17, 2000, as amended at 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

#### **§ 162.1602 Standards for health care electronic funds transfers (EFT) and remittance advice transaction.**

The Secretary adopts the following standards:

(a) For the period from October 16, 2003 through March 16, 2009: Health care claims and remittance advice. The ASC X12N 835—Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, and Addenda to Health Care Claim Payment/Advice, Version 4010, October 2002, Washington Publishing Company, 004010X091A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both of the following standards:

(1) The standard identified in paragraph (a) of this section.

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920.)

(c) For the period from January 1, 2012 through December 31, 2013, the standard identified in paragraph (b)(2) of this section.

(d) For the period on and after January 1, 2014, the following standards:

(1) Except when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, for Stage 1 Payment Initiation transmissions described in § 162.1601(a), all of the following standards:

(i) The National Automated Clearing House Association (NACHA) Corporate Credit or Deposit Entry with Addenda Record (CCD+) implementation specifications as contained in the 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network as follows (incorporated by reference in § 162.920)—

(A) NACHA Operating Rules, Appendix One: ACH File Exchange Specifications; and

(B) NACHA Operating Rules, Appendix Three: ACH Record Format Specifications, Subpart 3.1.8 Sequence of Records for CCD Entries.

(ii) For the CCD Addenda Record (“7”), field 3, of the

standard identified in 1602(d)(1)(i), the Accredited Standards Committee (ASC) X12 Standards for Electronic Data Interchange Technical Report Type 3, "Health Care Claim Payment/Advice (835), April 2006: Section 2.4: 835 Segment Detail: "TRN Reassociation Trace Number," Washington Publishing Company, 005010X221 (Incorporated by reference in § 162.920).

(2) For transmissions described in § 162.1601(b), including when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, "Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920).

[77 FR 1590, Jan. 10, 2012]

**§ 162.1603 Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction.**

On and after January 1, 2014, the Secretary adopts the following for the health care electronic funds transfers (EFT) and remittance advice transaction:

(a) The Phase III CORE EFT & ERA Operating Rule Set, Approved June 2012 (Incorporated by reference in § 162.920) which includes the following rules:

(1) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(2) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(3) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(4) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(5) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(6) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled "Health Care Claim Payment/Advice Batch Acknowledgement Requirements".

(b) ACME Health Plan, CORE v5010 Master Companion Guide Template, 005010, 1.2, March 2011 (incorporated by reference in § 162.920), as required by the Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012.

[77 FR 48043, Aug. 10, 2012]

**Subpart Q—Health Plan Premium Payments**

**§ 162.1701 Health plan premium payments transaction.**

The health plan premium payment transaction is the transmission of any of the

following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit health care premium payments including any of the following:

(1) Payroll deductions.

(2) Other group premium payments.

(3) Associated group premium payment information.

**§ 162.1702 Standards for health plan premium payments transaction.**

The Secretary adopts the following standards for the health plan premium payments transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N 820—Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, and Addenda to Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, October 2002, Washington Publishing Company, 004010X061A1.

(Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section, and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007, ASC X12N/005010X218. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

### **Subpart R—Coordination of Benefits**

#### **§ 162.1801 Coordination of benefits transaction.**

The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care:

(a) Claims.

(b) Payment information.

#### **§ 162.1802 Standards for coordination of benefits information transaction.**

The Secretary adopts the following standards for the

coordination of benefits information transaction.

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drug claims*. The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental health care claims*. The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims*. The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims*. The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drug claims*. The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837), ASC X12 Standards for Electronic Date Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222.



(Incorporated by reference in § 162.920.)

(iv) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8399, Feb. 20, 2003, as amended at 74 FR 3327, Jan. 16, 2009]

#### **Subpart S—Medicaid Pharmacy Subrogation**

SOURCE: 74 FR 3328, Jan. 16, 2009, unless otherwise noted.

#### **§ 162.1901 Medicaid pharmacy subrogation transaction.**

The Medicaid pharmacy subrogation transaction is the transmission of a claim from a Medicaid agency to a payer for the purpose of seeking reimbursement from the responsible health plan for a pharmacy claim the State has paid on behalf of a Medicaid recipient.

#### **§ 162.1902 Standard for Medicaid pharmacy subrogation transaction.**

The Secretary adopts the Batch Standard Medicaid Subrogation

Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902 (Incorporated by reference at § 162.920):

(a) For the period on and after January 1, 2012, for covered entities that are not small health plans;

(b) For the period on and after January 1, 2013 for small health plans.

---

**PART 164—SECURITY AND  
PRIVACY**

---

**Contents**

Subpart A—General Provisions

§ 164.102 Statutory basis.  
§ 164.103 Definitions.  
§ 164.104 Applicability.  
§ 164.105 Organizational requirements.  
§ 164.106 Relationship to other parts.

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability.  
§ 164.304 Definitions.  
§ 164.306 Security standards: General rules.  
§ 164.308 Administrative safeguards.  
§ 164.310 Physical safeguards.  
§ 164.312 Technical safeguards.  
§ 164.314 Organizational requirements.  
§ 164.316 Policies and procedures and documentation requirements.  
§ 164.318 Compliance dates for the initial implementation of the security standards.  
Appendix A to Subpart C of Part 164—Security Standards: Matrix

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

§ 164.400 Applicability.  
§ 164.402 Definitions.  
§ 164.404 Notification to individuals.  
§ 164.406 Notification to the

media.  
§ 164.408 Notification to the Secretary.  
§ 164.410 Notification by a business associate.  
§ 164.412 Law enforcement delay.  
§ 164.414 Administrative requirements and burden of proof.

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.  
§ 164.501 Definitions.  
§ 164.502 Uses and disclosures of protected health information: general rules.  
§ 164.504 Uses and disclosures: Organizational requirements.  
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.  
§ 164.508 Uses and disclosures for which an authorization is required.  
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.  
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.  
§ 164.514 Other requirements relating to uses and disclosures of protected health information.  
§ 164.520 Notice of privacy practices for protected health information.  
§ 164.522 Rights to request privacy protection for protected health information.  
§ 164.524 Access of individuals to protected health information.  
§ 164.526 Amendment of protected health information.  
§ 164.528 Accounting of disclosures of protected health information.  
§ 164.530 Administrative requirements.

§ 164.532 Transition provisions.  
§ 164.534 Compliance dates for initial implementation of the privacy standards.

---

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

**Subpart A—General Provisions**

**§ 164.102 Statutory basis.**

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and sections 13400-13424 of Public Law 111-5.

[78 FR 5692, Jan. 25, 2013]

**§ 164.103 Definitions.**

As used in this part, the following terms have the following meanings:

*Common control* exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

*Common ownership* exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

*Covered functions* means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

*Health care component* means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).

*Hybrid entity* means a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D).

*Law enforcement official* means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of law; or
- (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

*Plan sponsor* is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

*Required by law* means a mandate contained in law that compels an entity to make a use

or disclosure of protected health information and that is enforceable in a court of law.

*Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009]

#### § 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

#### § 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(B) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse,” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to “electronic protected health information” refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's

work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section

for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

#### **§ 164.106 Relationship to other parts.**

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

#### **Subpart B [Reserved]**

#### **Subpart C—Security Standards for the Protection of Electronic Protected Health Information**

AUTHORITY: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

#### **§ 164.302 Applicability.**

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

#### **§ 164.304 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in this subpart, not as used in subparts D or E of this part.)

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

*Authentication* means the corroboration that a person is the one claimed.

*Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control

that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Security or Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

**§ 164.306 Security standards: General rules.**

*(a) General requirements.*

Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

*(b) Flexibility of approach.*

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation

specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of

electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

**§ 164.308 Administrative safeguards.**

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision (Addressable).* Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions (Required).* If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization (Addressable).* Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right

of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training.*

Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders (Addressable).* Periodic security updates.

(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management (Addressable).* Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based

initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that



meets the applicable requirements of § 164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.310 Physical safeguards.**

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations (Addressable).* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan (Addressable).* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures (Addressable).* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to

software programs for testing and revision.

(iv) *Maintenance records (Addressable).* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal (Required).* Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use (Required).* Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable).* Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable).* Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.312 Technical safeguards.**

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required)*. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)*. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable)*. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

#### **§ 164.314 Organizational requirements.**

(a)(1) *Standard: Business associate contracts or other arrangements*. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required)*.

(i) *Business associate contracts*. The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) *Other arrangements*. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors*. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) *Standard: Requirements for group health plans*. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected

health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

*(2) Implementation specifications (Required).* The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.316 Policies and procedures and documentation requirements.**

A covered entity or business associate must, in accordance with § 164.306:

*(a) Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

*(b)(1) Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

*(2) Implementation specifications:*

(i) *Time limit (Required).* Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required).* Make documentation available to those persons responsible for implementing the procedures to

which the documentation pertains.

(iii) *Updates (Required).* Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

**§ 164.318 Compliance dates for the initial implementation of the security standards.**

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

**Appendix A to Subpart C of Part  
 164—Security Standards: Matrix**

<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)=Required, (A)=Addressable</b>
<b>Administrative Safeguards</b>		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
<b>Physical Safeguards</b>		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
<b>Technical Safeguards(see § 164.312)</b>		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

**Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

**§ 164.400 Applicability.**

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

**§ 164.402 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or

disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

*Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

[78 FR 5695, Jan. 25, 2013]

**§ 164.404 Notification to individuals.**

(a) *Standard* —(1) *General rule.* A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification* —(1) *Elements.* The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the

breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) *Plain language requirement.* The notification required by paragraph (a) of this section shall be written in plain language.

(d) *Implementation specifications: Methods of individual notification.* The notification required by paragraph (a) of this section shall be provided in the following form:

(1) *Written notice.* (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as

specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) *Substitute notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) *Additional notice in urgent situations.* In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

#### **§ 164.406 Notification to the media.**

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

#### **§ 164.408 Notification to the Secretary.**

(a) *Standard.* A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) *Implementation specifications: Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

**§ 164.410 Notification by a business associate.**

(a) *Standard*—(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach

is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) *Implementation specifications: Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

**§ 164.412 Law enforcement delay.**

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

**§ 164.414 Administrative requirements and burden of proof.**

(a) *Administrative requirements.* A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

**Subpart E—Privacy of Individually Identifiable Health Information**

AUTHORITY: 42 U.S.C. 1320d-2, 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

**§ 164.500 Applicability.**

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of



this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

(d) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5695, Jan. 25, 2013]

#### § 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

*Correctional institution* means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal

justice system, witnesses, or others awaiting charges or trial.

*Data aggregation* means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

*Designated record set* means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

*Direct treatment relationship* means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

*Health care operations* means any of the following activities of the covered entity to the extent that the

activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud

and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

*Health oversight agency* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from

or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

*Indirect treatment relationship* means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

*Inmate* means a person incarcerated in or otherwise confined to a correctional institution.

*Marketing:* (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is

reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

*Payment* means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

*Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

*Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

*Public health authority* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

*Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

*Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 42769, Aug. 24, 2009; 78 FR 5695, Jan. 25, 2013]

**§ 164.502 Uses and disclosures of protected health information: General rules.**

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i),

pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures.*

(i) *Use and disclosure of genetic information for underwriting purposes:* Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

(ii) *Sale of protected health information:*

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(2) Sale of protected health information does not include a disclosure of protected health information:

(i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(iii) For treatment and payment purposes pursuant to § 164.506(a);

(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(vi) To an individual, when requested under § 164.524 or § 164.528;

(vii) Required by law as permitted under § 164.512(a); and

(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(b) *Standard: Minimum necessary*

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the

minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that

is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.*, de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the

subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)(i) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an

individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has

engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 78 FR 5696, Jan. 25, 2013]

**§ 164.504 Uses and disclosures:  
Organizational requirements.**

(a) *Definitions.* As used in this section:

*Plan administration functions* means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

*Summary health information* means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)-(d) [Reserved]

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable

steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.



(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the

business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health

information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(I) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such

information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation

specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5697, Jan. 25, 2013]

**§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.**

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.*

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is

required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.* (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5698, Jan. 25, 2013]

**§ 164.508 Uses and disclosures for which an authorization is required.**

(a) *Standard: Authorizations for uses and disclosures* —(1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: Psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a);

§ 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) *Authorization required: Sale of protected health information.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart.  
(ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) *Implementation specifications: General requirements*

(1) *Valid authorizations.*

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an

authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements*

(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including

for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health

plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5699, Jan. 25, 2013]

**§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.**

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: Use and disclosure for facility directories*

(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Use or disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.* (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes*

(1) *Permitted uses and disclosures.*

(i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health

information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013]

**§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.**

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure

permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: Uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: Uses and disclosures for public health activities.* (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity

for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:



(1) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the

individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: Uses and disclosures for health oversight activities*

(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal

proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: Disclosures for judicial and administrative proceedings*

(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory

assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for

disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a

law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith

constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: Reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: Uses and disclosures about decedents.*

(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health

information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: Uses and disclosures for research purposes*

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34

CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(1) An adequate plan to protect the identifiers from improper use and disclosure;

(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized

oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety*

(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.*

(1) *Military and veterans activities*

(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.*, Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual

was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

- (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;
- (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
- (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.*

(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

- (A) The provision of health care to such individuals;
- (B) The health and safety of such individual or other inmates;
- (C) The health and safety of the officers or employees of or others at the correctional institution;
- (D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.*

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered

functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

**§ 164.514 Other requirements relating to uses and disclosures of protected health information.**

(a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with

other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: Re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and

is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: Minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: Minimum necessary uses of protected health information.*

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.*

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must



implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.*

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2)

and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

*(3) Implementation specification: Permitted purposes for uses and disclosures.*

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

*(4) Implementation specifications: Data use agreement*

(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

*(iii) Compliance.*

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

*(f) Fundraising communications.*

(1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) *Implementation specifications: Fundraising requirements.* (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the

individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.*

(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health

information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are

met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

**§ 164.520 Notice of privacy practices for protected health information.**

(a) *Standard: notice of privacy practices.*

(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary

health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: Content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED

AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications;

(B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to

make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.*

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii),

the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.*

(i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided

to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

**§ 164.522 Rights to request privacy protection for protected health information.**

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(vi) A covered entity must agree to the request of an individual to restrict

disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

(b)(1) *Standard: Confidential communications requirements.*

(i) A covered health care provider must permit individuals to request

and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

**§ 164.524 Access of individuals to protected health information.**

(a) *Standard: Access to protected health information.*

(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.



(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by

paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: Requests for access and timely action.*

(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the

protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.* (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with

access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access

to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

[65 FR 82823, Dec. 28, 2000, as amended at 78 FR 5701, Jan. 25, 2013]

**§ 164.526 Amendment of protected health information.**

(a) *Standard: Right to amend.* (1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: Requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record

set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the

covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered

entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.* (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

**§ 164.528 Accounting of disclosures of protected health information.**

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- (i) To carry out treatment, payment and health care operations as provided in § 164.506;
- (ii) To individuals of protected health information about them as provided in § 164.502;
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
- (iv) Pursuant to an authorization as provided in § 164.508;
- (v) For the facility's directory or to persons involved in the individual's

care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

- (i) The date of the disclosure;
- (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the

same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to

whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

#### **§ 164.530 Administrative requirements.**

(a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in

paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the

covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in § 160.316 of this subchapter.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures

with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies and procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's

policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation



required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 71 FR 8433, Feb. 16, 2006; 74 FR 42769, Aug. 24, 2009]

### § 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained

from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) *Effect of prior data use agreements.* If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 78 FR 5702, Jan. 25, 2013]

**§ 164.534 Compliance dates for initial implementation of the privacy standards.**

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) *Health plans other than small health plans.* April 14, 2003.

(2) *Small health plans.* April 14, 2004.

(c) *Health clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

5



**OCR PRIVACY BRIEF**

# **SUMMARY OF THE HIPAA PRIVACY RULE**



**HIPAA Compliance Assistance**

# SUMMARY OF THE HIPAA PRIVACY RULE

## Contents

Introduction .....	1
Statutory & Regulatory Background.....	1
Who is Covered by the Privacy Rule .....	2
Business Associates.....	3
What Information is Protected .....	3
General Principle for Uses and Disclosures.....	4
Permitted Uses and Disclosures .....	4
Authorized Uses and Disclosures.....	9
Limiting Uses and Disclosures to the Minimum Necessary.....	10
Notice and Other Individual Rights .....	11
Administrative Requirements.....	14
Organizational Options .....	15
Other Provisions: Personal Representatives and Minors .....	16
State Law.....	17
Enforcement and Penalties for Noncompliance.....	17
Compliance Dates .....	18
Copies of the Rule & Related Materials.....	18
End Notes .....	19

# SUMMARY OF THE HIPAA PRIVACY RULE

<p><b>Introduction</b></p>	<p>The <i>Standards for Privacy of Individually Identifiable Health Information</i> (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).<sup>1</sup> The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.</p> <p>A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.</p> <p>This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: <a href="http://www.hhs.gov/ocr/hipaa">http://www.hhs.gov/ocr/hipaa</a>. In the event of a conflict between this summary and the Rule, the Rule governs.</p> <p>Links to the OCR Guidance Document are provided throughout this paper. Provisions of the Rule referenced in this summary are cited in endnotes at the end of this document. To review the entire Rule itself, and for other additional helpful information about how it applies, see the OCR website: <a href="http://www.hhs.gov/ocr/hipaa">http://www.hhs.gov/ocr/hipaa</a>.</p>
<p><b>Statutory &amp; Regulatory Background</b></p>	<p>The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the <i>Administrative Simplification</i> provisions.</p> <p>HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within</p>

	<p>three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.<sup>2</sup></p> <p>In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.<sup>3</sup> A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website: <a href="http://www.hhs.gov/ocr/hipaa">http://www.hhs.gov/ocr/hipaa</a>.</p>
<p><b>Who is Covered by the Privacy Rule</b></p>	<p>The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the “covered entities”). For help in determining whether you are covered, use the decision tool at: <a href="http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp">http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp</a>.</p> <p><b>Health Plans.</b> Individual and group plans that provide or pay the cost of medical care are covered entities.<sup>4</sup> Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (“HMOs”), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,<sup>5</sup> or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers’ compensation, automobile insurance, and property and casualty insurance.</p> <p><b>Health Care Providers.</b> Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.<sup>6</sup> Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all “providers of services” (e.g., institutional providers such as hospitals) and “providers of medical or health services” (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.</p>

	<p><b>Health Care Clearinghouses.</b> <i>Health care clearinghouses</i> are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.<sup>7</sup> In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.<sup>8</sup> Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.</p>
<p><b>Business Associates</b></p>	<p><b>Business Associate Defined.</b> In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.<sup>9</sup> Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.</p> <p><b>Business Associate Contract.</b> When a covered entity uses a contractor or other non-workforce member to perform "<i>business associate</i>" services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.<sup>10</sup> Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.<sup>11</sup> Sample business associate contract language is available on the OCR website at: <a href="http://www.hhs.gov/ocr/hipaa/contractprov.html">http://www.hhs.gov/ocr/hipaa/contractprov.html</a>. Also see <a href="#">OCR "Business Associate" Guidance</a>.</p>
<p><b>What Information is Protected</b></p>	<p><b>Protected Health Information.</b> The Privacy Rule protects all "<i>individually identifiable health information</i>" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "<i>protected health information (PHI)</i>."<sup>12</sup></p>



	<p>“<i>Individually identifiable health information</i>” is information, including demographic data, that relates to:</p> <ul style="list-style-type: none"> <li>• the individual’s past, present or future physical or mental health or condition,</li> <li>• the provision of health care to the individual, or</li> <li>• the past, present, or future payment for the provision of health care to the individual,</li> </ul> <p>and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.<sup>13</sup> Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).</p> <p>The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.</p> <p><b>De-Identified Health Information.</b> There are no restrictions on the use or disclosure of de-identified health information.<sup>14</sup> De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.<sup>15</sup></p>
<p><b>General Principle for Uses and Disclosures</b></p>	<p><b>Basic Principle.</b> A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing.<sup>16</sup></p> <p><b>Required Disclosures.</b> A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.<sup>17</sup> See <a href="#">OCR “Government Access” Guidance</a>.</p>
<p><b>Permitted Uses and Disclosures</b></p>	<p><b>Permitted Uses and Disclosures.</b> A covered entity is permitted, but not required, to use and disclose protected health information, without an individual’s authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and</p>

(6) Limited Data Set for the purposes of research, public health or health care operations.<sup>18</sup> Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

**(1) To the Individual.** A covered entity may disclose protected health information to the individual who is the subject of the information.

**(2) Treatment, Payment, Health Care Operations.** A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.<sup>19</sup> A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See [OCR “Treatment, Payment, Health Care Operations” Guidance](#).

*Treatment* is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.<sup>20</sup>

*Payment* encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual<sup>21</sup> and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

*Health care operations* are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.<sup>22</sup>

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.<sup>23</sup>

Obtaining “consent” (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.<sup>24</sup> The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

**(3) Uses and Disclosures with Opportunity to Agree or Object.** Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

***Facility Directories.*** It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.<sup>25</sup> The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

***For Notification and Other Purposes.*** A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care.<sup>26</sup> This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

**(4) Incidental Use and Disclosure.** The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.<sup>27</sup> See [OCR "Incidental Uses and Disclosures" Guidance](#).

**(5) Public Interest and Benefit Activities.** The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.<sup>28</sup> These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

***Required by Law.*** Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

statute, regulation, or court orders).<sup>29</sup>

**Public Health Activities.** Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.<sup>30</sup> See [OCR “Public Health” Guidance](#); [CDC Public Health and HIPAA Guidance](#).

**Victims of Abuse, Neglect or Domestic Violence.** In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.<sup>31</sup>

**Health Oversight Activities.** Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.<sup>32</sup>

**Judicial and Administrative Proceedings.** Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.<sup>33</sup>

**Law Enforcement Purposes.** Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official’s request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person’s death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.<sup>34</sup>

***Decedents.*** Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.<sup>35</sup>

***Cadaveric Organ, Eye, or Tissue Donation.*** Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.<sup>36</sup>

***Research.*** “Research” is any systematic investigation designed to develop or contribute to generalizable knowledge.<sup>37</sup> The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual’s authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals’ authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.<sup>38</sup> A covered entity also may use or disclose, without an individuals’ authorization, a limited data set of protected health information for research purposes (see discussion below).<sup>39</sup> See [OCR “Research” Guidance; NIH Protecting PHI in Research](#).

***Serious Threat to Health or Safety.*** Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.<sup>40</sup>

***Essential Government Functions.*** An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.<sup>41</sup>

	<p><b>Workers' Compensation.</b> Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.<sup>42</sup> See <a href="#">OCR "Workers' Compensation" Guidance</a>.</p> <p><b>(6) Limited Data Set.</b> A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.<sup>43</sup> A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.</p>
<p><b>Authorized Uses and Disclosures</b></p>	<p><b>Authorization.</b> A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.<sup>44</sup> A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.<sup>45</sup></p> <p>An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.</p> <p>All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.<sup>46</sup></p> <p><b>Psychotherapy Notes<sup>47</sup>.</b> A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions<sup>48</sup>:</p> <ul style="list-style-type: none"> <li>• The covered entity who originated the notes may use them for treatment.</li> <li>• A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.</li> </ul> <p><b>Marketing.</b> Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.<sup>49</sup> The Privacy Rule carves out the following health-related activities from this definition of marketing:</p> <ul style="list-style-type: none"> <li>• Communications to describe health-related products or services, or payment</li> </ul>

	<p>for them, provided by or included in a benefit plan of the covered entity making the communication;</p> <ul style="list-style-type: none"> <li>• Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan’s enrollees that add value to, but are not part of, the benefits plan;</li> <li>• Communications for treatment of the individual; and</li> <li>• Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.</li> </ul> <p>Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity’s provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity’s receipt of direct or indirect remuneration from a third party must reveal that fact. See <a href="#">OCR "Marketing" Guidance</a>.</p>
<p><b>Limiting Uses and Disclosures to the Minimum Necessary</b></p>	<p><b>Minimum Necessary.</b> A central aspect of the Privacy Rule is the principle of “minimum necessary” use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.<sup>50</sup> A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. See <a href="#">OCR “Minimum Necessary” Guidance</a>.</p> <p>The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual’s personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.</p> <p><b>Access and Uses.</b> For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of</p>

	<p>protected health information to which access is needed, and any conditions under which they need the information to do their jobs.</p> <p><b>Disclosures and Requests for Disclosures.</b> Covered entities must establish and implement policies and procedures (which may be standard protocols) for <i>routine, recurring disclosures, or requests for disclosures</i>, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.</p> <p><b>Reasonable Reliance.</b> If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity’s business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.</p>
<p><b>Notice and Other Individual Rights</b></p>	<p><b>Privacy Practices Notice.</b> Each covered entity, with certain exceptions, must provide a notice of its privacy practices.<sup>51</sup> The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity’s duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals’ rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See <a href="#">OCR “Notice” Guidance</a>.</p> <ul style="list-style-type: none"> <li>• <b>Notice Distribution.</b> A covered health care provider with a <i>direct treatment relationship</i> with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: <ul style="list-style-type: none"> <li>○ Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);</li> <li>○ By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and</li> <li>○ In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.</li> </ul> </li> </ul>



Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.<sup>52</sup> A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.<sup>53</sup> Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the “named insured,” that is, the subscriber for coverage that also applies to spouses and dependents.

- **Acknowledgement of Notice Receipt.** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.<sup>54</sup> The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient’s written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

**Access.** Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity’s *designated record set*.<sup>55</sup> The “designated record set” is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider’s medical and billing records about individuals or a health plan’s enrollment, payment, claims adjudication, and case or medical management record systems.<sup>56</sup> The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.<sup>57</sup> Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

**Amendment.** The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is

inaccurate or incomplete.<sup>58</sup> If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.<sup>59</sup> If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

**Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.<sup>60</sup> The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

**Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.<sup>61</sup> A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.<sup>62</sup>

**Confidential Communications Requirements.** Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.<sup>63</sup> For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

## Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

**Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.<sup>64</sup>

**Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.<sup>65</sup>

**Workforce Training and Management.** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).<sup>66</sup> A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.<sup>67</sup> A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.<sup>68</sup>

**Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.<sup>69</sup>

**Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.<sup>70</sup> For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See [OCR "Incidental Uses and Disclosures" Guidance](#).

**Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.<sup>71</sup> The covered entity must explain those procedures in its privacy practices notice.<sup>72</sup>

Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

**Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.<sup>73</sup> A covered entity may not

	<p>require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.<sup>74</sup></p> <p><b>Documentation and Record Retention.</b> A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.<sup>75</sup></p> <p><b>Fully-Insured Group Health Plan Exception.</b> The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.<sup>76</sup></p>
<p><b>Organizational Options</b></p>	<p>The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections.</p> <p><b>Hybrid Entity.</b> The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a “hybrid entity.”<sup>77</sup> (The activities that make a person or organization a covered entity are its “covered functions.”<sup>78</sup>) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more “health care components.” After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule.</p> <p><b>Affiliated Covered Entity.</b> Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.<sup>79</sup> The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.</p> <p><b>Organized Health Care Arrangement.</b> The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as “organized health care arrangements.”<sup>80</sup> Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement’s joint health care operations.<sup>81</sup></p> <p><b>Covered Entities With Multiple Covered Functions.</b> A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.<sup>82</sup> The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.</p>

	<p><b>Group Health Plan disclosures to Plan Sponsors.</b> A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the “plan sponsor”—the employer, union, or other employee organization that sponsors and maintains the group health plan<sup>83</sup>:</p> <ul style="list-style-type: none"> <li>• Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan.</li> <li>• If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. “Summary health information” is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information).</li> <li>• Protected health information of the group health plan’s enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor’s use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.</li> </ul>
<p><b>Other Provisions: Personal Representatives and Minors</b></p>	<p><b>Personal Representatives.</b> The Privacy Rule requires a covered entity to treat a “<i>personal representative</i>” the same as the individual, with respect to uses and disclosures of the individual’s protected health information, as well as the individual’s rights under the Rule.<sup>84</sup> A personal representative is a person legally authorized to make health care decisions on an individual’s behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.</p> <p><b>Special case: Minors.</b> In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor’s protected health information, a covered entity has discretion to provide or deny a parent access to the minor’s health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See <a href="#">OCR “Personal Representatives” Guidance</a>.</p>

<p><b>State Law</b></p>	<p><b>Preemption.</b> In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.<sup>85</sup> “Contrary” means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.<sup>86</sup> The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits.</p> <p><b>Exception Determination.</b> In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law:</p> <ul style="list-style-type: none"> <li>• Is necessary to prevent fraud and abuse related to the provision of or payment for health care,</li> <li>• Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,</li> <li>• Is necessary for State reporting on health care delivery or costs,</li> <li>• Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or</li> <li>• Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.</li> </ul>
<p><b>Enforcement and Penalties for Noncompliance</b></p>	<p><b>Compliance.</b> Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.<sup>87</sup> The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews.</p> <p><b>Civil Money Penalties.</b> HHS may impose civil money penalties on a covered entity of \$100 per failure to comply with a Privacy Rule requirement.<sup>88</sup> That penalty may not exceed \$25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.</p>

	<p><b>Criminal Penalties.</b> A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of \$50,000 and up to one-year imprisonment.<sup>89</sup> The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.</p>
<p><b>Compliance Dates</b></p>	<p><b>Compliance Schedule.</b> All covered entities, except “small health plans,” must be compliant with the Privacy Rule by April 14, 2003.<sup>90</sup> Small health plans, however, have until April 14, 2004 to comply.</p> <p><b>Small Health Plans.</b> A health plan with annual receipts of not more than \$5 million is a small health plan.<sup>91</sup> Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.<sup>92</sup> See <a href="#">What constitutes a small health plan?</a></p>
<p><b>Copies of the Rule &amp; Related Materials</b></p>	<p>The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, <a href="http://www.hhs.gov/ocr/hipaa">http://www.hhs.gov/ocr/hipaa</a>.</p>

## End Notes

---

<sup>1</sup> Pub. L. 104-191.

<sup>2</sup> 65 FR 82462.

<sup>3</sup> 67 FR 53182.

<sup>4</sup> 45 C.F.R. §§ 160.102, 160.103.

<sup>5</sup> Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

<sup>6</sup> 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

<sup>7</sup> 45 C.F.R. § 160.103.

<sup>8</sup> 45 C.F.R. § 164.500(b).

<sup>9</sup> 45 C.F.R. § 160.103.

<sup>10</sup> 45 C.F.R. §§ 164.502(e), 164.504(e).

<sup>11</sup> 45 C.F.R. § 164.532

<sup>12</sup> 45 C.F.R. § 160.103.

<sup>13</sup> 45 C.F.R. § 160.103

<sup>14</sup> 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

<sup>15</sup> The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the “safe harbor” method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

<sup>16</sup> 45 C.F.R. § 164.502(a).

<sup>17</sup> 45 C.F.R. § 164.502(a)(2).



---

<sup>18</sup> 45 C.F.R. § 164.502(a)(1).

<sup>19</sup> 45 C.F.R. § 164.506(c).

<sup>20</sup> 45 C.F.R. § 164.501.

<sup>21</sup> 45 C.F.R. § 164.501.

<sup>22</sup> 45 C.F.R. § 164.501.

<sup>23</sup> 45 C.F.R. § 164.508(a)(2)

<sup>24</sup> 45 C.F.R. § 164.506(b).

<sup>25</sup> 45 C.F.R. § 164.510(a).

<sup>26</sup> 45 C.F.R. § 164.510(b).

<sup>27</sup> 45 C.F.R. §§ 164.502(a)(1)(iii).

<sup>28</sup> *See* 45 C.F.R. § 164.512.

<sup>29</sup> 45 C.F.R. § 164.512(a).

<sup>30</sup> 45 C.F.R. § 164.512(b).

<sup>31</sup> 45 C.F.R. § 164.512(a), (c).

<sup>32</sup> 45 C.F.R. § 164.512(d).

<sup>33</sup> 45 C.F.R. § 164.512(e).

<sup>34</sup> 45 C.F.R. § 164.512(f).

<sup>35</sup> 45 C.F.R. § 164.512(g).

<sup>36</sup> 45 C.F.R. § 164.512(h).

<sup>37</sup> The Privacy Rule defines research as, “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” 45 C.F.R. § 164.501.

<sup>38</sup> 45 C.F.R. § 164.512(i).

<sup>39</sup> 45 CFR § 164.514(e).

<sup>40</sup> 45 C.F.R. § 164.512(j).

<sup>41</sup> 45 C.F.R. § 164.512(k).

<sup>42</sup> 45 C.F.R. § 164.512(l).

<sup>43</sup> 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

<sup>44</sup> 45 C.F.R. § 164.508.

<sup>45</sup> A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the

---

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

<sup>46</sup> 45 CFR § 164.532.

<sup>47</sup> "Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

<sup>48</sup> 45 C.F.R. § 164.508(a)(2).

<sup>49</sup> 45 C.F.R. §§ 164.501 and 164.508(a)(3).

<sup>50</sup> 45 C.F.R. §§ 164.502(b) and 164.514 (d).

<sup>51</sup> 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

<sup>52</sup> 45 C.F.R. § 164.520(c).

<sup>53</sup> 45 C.F.R. § 164.520(d).

<sup>54</sup> 45 C.F.R. § 164.520(c).

<sup>55</sup> 45 C.F.R. § 164.524.

<sup>56</sup> 45 C.F.R. § 164.501.

<sup>57</sup> A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

---

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

<sup>58</sup> 45 C.F.R. § 164.526.

<sup>59</sup> Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

<sup>60</sup> 45 C.F.R. § 164.528.

<sup>61</sup> 45 C.F.R. § 164.522(a).

<sup>62</sup> 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

<sup>63</sup> 45 C.F.R. § 164.522(b).

<sup>64</sup> 45 C.F.R. § 164.530(i).

<sup>65</sup> 45 C.F.R. § 164.530(a).

<sup>66</sup> 45 C.F.R. § 160.103.

<sup>67</sup> 45 C.F.R. § 164.530(b).

<sup>68</sup> 45 C.F.R. § 164.530(e).

<sup>69</sup> 45 C.F.R. § 164.530(f).

<sup>70</sup> 45 C.F.R. § 164.530(c).

<sup>71</sup> 45 C.F.R. § 164.530(d).

<sup>72</sup> 45 C.F.R. § 164.520(b)(1)(vi).

<sup>73</sup> 45 C.F.R. § 164.530(g).

<sup>74</sup> 45 C.F.R. § 164.530(h).

<sup>75</sup> 45 C.F.R. § 164.530(j).

<sup>76</sup> 45 C.F.R. § 164.530(k).

<sup>77</sup> 45 C.F.R. §§ 164.103, 164.105.

<sup>78</sup> 45 C.F.R. § 164.103.

<sup>79</sup> 45 C.F.R. § 164.105. Common ownership exists if an entity possesses an ownership or equity interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

<sup>80</sup> The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

---

utilization review, quality assessment and improvement activities, or risk-sharing payment activities.

- A group health plan and the health insurer or HMO that insures the plan's benefits, with respect to protected health information created or received by the insurer or HMO that relates to individuals who are or have been participants or beneficiaries of the group health plan.
- All group health plans maintained by the same plan sponsor.
- All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans' benefits, with respect to protected health information created or received by the insurers or HMOs that relates to individuals who are or have been participants or beneficiaries in the group health plans.

<sup>81</sup> 45 C.F.R. § 164.506(c)(5).

<sup>82</sup> 45 C.F.R. § 164.504(g).

<sup>83</sup> 45 C.F.R. § 164.504(f).

<sup>84</sup> 45 C.F.R. § 164.502(g).

<sup>85</sup> 45 C.F.R. § 160.203.

<sup>86</sup> 45 C.F.R. § 160.202.

<sup>87</sup> 45 C.F.R. § 160.304

<sup>88</sup> Pub. L. 104-191; 42 U.S.C. § 1320d-5.

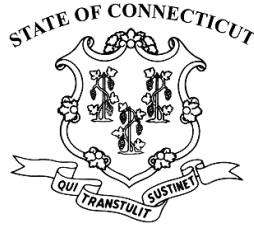
<sup>89</sup> Pub. L. 104-191; 42 U.S.C. § 1320d-6.

<sup>90</sup> 45 C.F.R. § 164.534.

<sup>91</sup> 45 C.F.R. § 160.103.

<sup>92</sup> Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine proxy measures to determine their total annual receipts.

6



**Substitute Senate Bill No. 3**

**Public Act No. 23-56**

**AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS.**

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 42-515 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

As used in this section and sections 42-516 to 42-525, inclusive, as amended by this act, and section 2 of this act, unless the context otherwise requires:

(1) "Abortion" means terminating a pregnancy for any purpose other than producing a live birth.

~~[(1)]~~ (2) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" [or] and "controlled" [means] mean (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

**Substitute Senate Bill No. 3**

[(2)] (3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 42-518 is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

[(3)] (4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

[(4)] (5) "Business associate" has the same meaning as provided in HIPAA.

[(5)] (6) "Child" has the same meaning as provided in COPPA.

[(6)] (7) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

[(7)] (8) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or

**Substitute Senate Bill No. 3**

contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(9) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

(10) "Consumer health data controller" means any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

[(8)] (11) "Controller" means [an individual] a person who, [or legal entity that,] alone or jointly with others, determines the purpose and means of processing personal data.

[(9)] (12) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

[(10)] (13) "Covered entity" has the same meaning as provided in HIPAA.

[(11)] (14) "Dark pattern" [(A)] means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and [(B)] includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

[(12)] (15) "Decisions that produce legal or similarly significant effects



**Substitute Senate Bill No. 3**

concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

[(13)] (16) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(17) "Gender-affirming health care services" has the same meaning as provided in section 52-571n.

(18) "Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

(19) "Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary.

[(14)] (20) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

[(15)] (21) "Identified or identifiable individual" means an individual

**Substitute Senate Bill No. 3**

who can be readily identified, directly or indirectly.

[(16)] (22) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(23) "Mental health facility" means any health care facility in which at least seventy per cent of the health care services provided in such facility are mental health services.

[(17)] (24) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

(25) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

[(18)] (26) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

[(19)] (27) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

**Substitute Senate Bill No. 3**

[(20)] (28) "Process" [or] and "processing" [means] mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

[(21)] (29) "Processor" means [an individual] a person who [, or legal entity that,] processes personal data on behalf of a controller.

[(22)] (30) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

[(23)] (31) "Protected health information" has the same meaning as provided in HIPAA.

[(24)] (32) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

[(25)] (33) "Publicly available information" means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(34) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning

**Substitute Senate Bill No. 3**

(A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment, (B) a social, psychological, behavioral or medical intervention, (C) a surgery or procedure, including, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

(35) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(36) "Reproductive or sexual health facility" means any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care.

~~[(26)]~~ (37) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or

**Substitute Senate Bill No. 3**

other transaction, in which the third party assumes control of all or part of the controller's assets.

[(27)] (38) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) consumer health data, (C) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, [(C)] (D) personal data collected from a known child, [or (D)] (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, or (F) precise geolocation data.

[(28)] (39) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

[(29)] (40) "Third party" means [an individual or legal entity] a person, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

[(30)] (41) "Trade secret" has the same meaning as provided in section 35-51.

Sec. 2. (NEW) (*Effective July 1, 2023*) (a) (1) Except as provided in

***Substitute Senate Bill No. 3***

subsection (b) of this section, subsections (b) and (c) of section 42-517 of the general statutes, as amended by this act, and section 42-524 of the general statutes, as amended by this act, no person shall: (A) Provide any employee or contractor with access to consumer health data unless the employee or contractor is subject to a contractual or statutory duty of confidentiality; (B) provide any processor with access to consumer health data unless such person and processor comply with section 42-521 of the general statutes; (C) use a geofence to establish a virtual boundary that is within one thousand seven hundred fifty feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data; or (D) sell, or offer to sell, consumer health data without first obtaining the consumer's consent.

(2) Notwithstanding section 42-516 of the general statutes, the provisions of subsection (a) of this section, and the provisions of section 42-515, as amended by this act, and sections 42-517 to 42-525, inclusive, of the general statutes, as amended by this act, concerning consumer health data and consumer health data controllers, apply to persons that conduct business in this state and persons that produce products or services that are targeted to residents of this state.

(b) The provisions of subsection (a) of this section shall not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in subdivision (1) of this subsection while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5)

### **Substitute Senate Bill No. 3**

financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; (6) covered entity or business associate, as defined in 45 CFR 160.103; (7) tribal nation government organization; or (8) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

Sec. 3. Subsections (a) to (c), inclusive, of section 42-517 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) The provisions of sections 42-515 to 42-525, inclusive, as amended by this act, do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in subdivision (1) of this subsection while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract; (3) nonprofit organization; [(3)] (4) institution of higher education; [(4)] (5) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; [(5)] (6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; [or (6)] (7) covered entity or business associate, as defined in 45 CFR 160.103; (8) tribal nation government organization; or (9) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(b) The following information and data is exempt from the provisions of sections 42-515 to 42-525, inclusive, as amended by this act, and

**Substitute Senate Bill No. 3**

section 2 of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health [care related] care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such



**Substitute Senate Bill No. 3**

activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, consumer health data controller or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the [Airline Deregulation Act] Federal Aviation Act of 1958, 49 USC 40101 et seq., [as amended from time to time, by an air carrier subject to said act, to the extent sections 42-515 to 42-525, inclusive, are preempted by] and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) Controllers, [and] processors and consumer health data controllers that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act.

**Substitute Senate Bill No. 3**

Sec. 4. Subsection (a) of section 42-520 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) A controller shall: (1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in sections 42-515 to 42-525, inclusive, as amended by this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue; (4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers; (6) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and (7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, [and] or wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 42-515 to 42-525, inclusive,

**Substitute Senate Bill No. 3**

as amended by this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

Sec. 5. Section 42-524 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to restrict a controller's, [or] processor's or consumer health data controller's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that the controller, [or] processor or consumer health data controller reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) provide a product or service specifically requested by a consumer; (6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action; (10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the

**Substitute Senate Bill No. 3**

deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or consumer health data controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller or consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; (11) assist another controller, processor, consumer health data controller or third party with any of the obligations under sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act; or (12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers, [or] processors or consumer health data controllers under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not restrict a controller's, [or] processor's or consumer health data controller's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or consumer health data controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers, [or] processors or

**Substitute Senate Bill No. 3**

consumer health data controllers under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not apply where compliance by the controller, [or] processor or consumer health data controller with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to prevent a controller, [or] processor or consumer health data controller from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller, [or] processor or consumer health data controller that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller, [or] processor or consumer health data controller disclosed such personal data, the disclosing controller, [or] processor or consumer health data controller did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller, [or] processor or consumer health data controller in compliance with sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act is likewise not in violation of said sections for the transgressions of the controller, [or] processor or consumer health data controller from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to: (1) Impose any obligation on a controller, [or] processor or consumer health data controller that adversely affects the rights or freedoms of any person,

**Substitute Senate Bill No. 3**

including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t; or (2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller or consumer health data controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(g) If a controller or consumer health data controller processes personal data pursuant to an exemption in this section, the controller or consumer health data controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller or consumer health data controller with respect to such processing.

Sec. 6. Section 42-525 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) The Attorney General shall have exclusive authority to enforce violations of sections 42-515 to 42-524, inclusive, as amended by this act,

**Substitute Senate Bill No. 3**

and section 2 of this act.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 42-515 to 42-524, inclusive, as amended by this act, and section 2 of this act, issue a notice of violation to the controller or consumer health data controller if the Attorney General determines that a cure is possible. If the controller or consumer health data controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing: (1) The number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations that were cured during the sixty-day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller, [or] processor or consumer health data controller the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller, [or] processor or consumer health data controller; (3) the nature and extent of the controller's, [or] processor's or consumer health data controller's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; [and] (6) whether such alleged violation was likely caused by human or technical error; and (7) the sensitivity of the data.

(d) Nothing in sections 42-515 to 42-524, inclusive, as amended by this act, or section 2 of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or

**Substitute Senate Bill No. 3**

any other law.

(e) A violation of the requirements of sections 42-515 to 42-524, inclusive, as amended by this act, or section 2 of this act shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g shall not apply to such violation.

Sec. 7. (NEW) (*Effective July 1, 2024*) (a) For the purposes of this section:

(1) "Authenticate" means to use reasonable means and make a commercially reasonable effort to determine whether a request to exercise any right afforded under subsection (b) of this section has been submitted by, or on behalf of, the minor who is entitled to exercise such right;

(2) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(3) "Minor" means any consumer who is younger than eighteen years of age;

(4) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(5) "Social media platform" (A) means a public or semi-public Internet-based service or application that (i) is used by a consumer in this state, (ii) is primarily intended to connect and allow users to socially interact within such service or application, and (iii) enables a user to (I) construct a public or semi-public profile for the purposes of signing into and using such service or application, (II) populate a public list of other users with whom the user shares a social connection within such service or application, and (III) create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms,



**Substitute Senate Bill No. 3**

or through a landing page or main feed that presents the user with content generated by other users, and (B) does not include a public or semi-public Internet-based service or application that (i) exclusively provides electronic mail or direct messaging services, (ii) primarily consists of news, sports, entertainment, interactive video games, electronic commerce or content that is preselected by the provider or for which any chat, comments or interactive functionality is incidental to, directly related to, or dependent on the provision of such content, or (iii) is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program; and

(6) "Unpublish" means to remove a social media platform account from public visibility.

(b) (1) Not later than fifteen business days after a social media platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to unpublish such minor's social media platform account, the social media platform shall unpublish such minor's social media platform account.

(2) Not later than forty-five business days after a social media platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to delete such minor's social media platform account, the social media platform shall delete such minor's social media platform account and cease processing such minor's personal data except where the preservation of such minor's social media platform account or personal data is otherwise permitted or required by applicable law, including, but not limited to, sections 42-515 to 42-525, inclusive, of the general statutes, as amended by this act. A social media platform may extend such forty-five business day period by an additional forty-five business days if such extension is reasonably necessary considering the complexity and number of the consumer's requests, provided the social media platform

**Substitute Senate Bill No. 3**

informs the minor or, if the minor is younger than sixteen years of age, such minor's parent or legal guardian within the initial forty-five business day response period of such extension and the reason for such extension.

(3) A social media platform shall establish, and shall describe in a privacy notice, one or more secure and reliable means for submitting a request pursuant to this subsection. A social media platform that provides a mechanism for a minor or, if the minor is younger than sixteen years of age, the minor's parent or legal guardian to initiate a process to delete or unpublish such minor's social media platform account shall be deemed to be in compliance with the provisions of this subsection.

(c) If a social media platform is unable to authenticate a request submitted under subsection (b) of this section, the social media platform shall (1) not be required to comply with such request, and (2) provide a notice to the consumer who submitted such request disclosing that such social media platform (A) is unable to authenticate such request, and (B) will not be able to authenticate such request until such consumer provides the additional information that is reasonably necessary to authenticate such request.

(d) Any violation of the provisions of this section shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 8. (NEW) (*Effective October 1, 2024*) For the purposes of this section and sections 9 to 13, inclusive, of this act:

(1) "Adult" means any individual who is at least eighteen years of age;

**Substitute Senate Bill No. 3**

(2) "Consent" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(3) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(4) "Controller" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(5) "Heightened risk of harm to minors" means processing minors' personal data in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, or (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person;

(6) "HIPAA" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(7) "Minor" means any consumer who is younger than eighteen years of age;

(8) "Online service, product or feature" means any service, product or feature that is provided online. "Online service, product or feature" does not include any (A) telecommunications service, as defined in 47 USC 153, as amended from time to time, (B) broadband Internet access service, as defined in 47 CFR 54.400, as amended from time to time, or (C) delivery or use of a physical product;

(9) "Person" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(10) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

**Substitute Senate Bill No. 3**

(11) "Precise geolocation data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(12) "Process" and "processing" have the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(13) "Processor" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(14) "Profiling" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(15) "Protected health information" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(16) "Sale of personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(17) "Targeted advertising" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act; and

(18) "Third party" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act.

Sec. 9. (NEW) (*Effective October 1, 2024*) (a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature. In any enforcement action brought by the Attorney General pursuant to section 13 of this act, there shall be a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with the provisions of section 10 of this act concerning data protection assessments.

**Substitute Senate Bill No. 3**

(b) (1) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall: (A) Process any minor's personal data (i) for the purposes of (I) targeted advertising, (II) any sale of personal data, or (III) profiling in furtherance of any fully automated decision made by such controller that produces any legal or similarly significant effect concerning the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services, (ii) unless such processing is reasonably necessary to provide such online service, product or feature, (iii) for any processing purpose (I) other than the processing purpose that the controller disclosed at the time such controller collected such personal data, or (II) that is reasonably necessary for, and compatible with, the processing purpose described in subparagraph (A)(iii)(I) of this subdivision, or (iv) for longer than is reasonably necessary to provide such online service, product or feature; or (B) use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature. The provisions of this subdivision shall not apply to any service or application that is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program.

(2) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers an online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall collect a minor's precise geolocation data unless: (A) Such precise geolocation data is reasonably necessary for the controller to provide such online service, product or feature and, if such data is necessary to provide such online service, product or feature, such controller may only collect such data for the

***Substitute Senate Bill No. 3***

time necessary to provide such online service, product or feature; and (B) the controller provides to the minor a signal indicating that such controller is collecting such precise geolocation data, which signal shall be available to such minor for the entire duration of such collection.

(3) No controller shall engage in the activities described in subdivisions (1) and (2) of this subsection unless the controller obtains the minor's consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time, shall be deemed to have satisfied any requirement to obtain parental consent under this subdivision.

(c) (1) No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall: (A) Provide any consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice; or (B) except as provided in subdivision (2) of this subsection, offer any direct messaging apparatus for use by minors without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to minors with whom they are not connected.

(2) The provisions of subparagraph (B) of subdivision (1) of this subsection shall not apply to services where the predominant or exclusive function is: (A) Electronic mail; or (B) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, where messages are (i) shared between the sender and the recipient, (ii) only visible to the sender and the recipient, and (iii) not

**Substitute Senate Bill No. 3**

posted publicly.

Sec. 10. (NEW) (*Effective October 1, 2024*) (a) Each controller that, on or after October 1, 2024, offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall conduct a data protection assessment for such online service, product or feature: (1) In a manner that is consistent with the requirements established in section 42-522 of the general statutes; and (2) that addresses (A) the purpose of such online service, product or feature, (B) the categories of minors' personal data that such online service, product or feature processes, (C) the purposes for which such controller processes minors' personal data with respect to such online service, product or feature, and (D) any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product or feature to minors.

(b) Each controller that conducts a data protection assessment pursuant to subsection (a) of this section shall: (1) Review such data protection assessment as necessary to account for any material change to the processing operations of the online service, product or feature that is the subject of such data protection assessment; and (2) maintain documentation concerning such data protection assessment for the longer of (A) the three-year period beginning on the date on which such processing operations cease, or (B) as long as such controller offers such online service, product or feature.

(c) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(d) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment

**Substitute Senate Bill No. 3**

that would otherwise be conducted pursuant to this section.

(e) If any controller conducts a data protection assessment pursuant to subsection (a) of this section and determines that the online service, product or feature that is the subject of such assessment poses a heightened risk of harm to minors, such controller shall establish and implement a plan to mitigate or eliminate such risk.

(f) Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to the attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

Sec. 11. (NEW) (*Effective October 1, 2024*) (a) A processor shall adhere to the instructions of a controller, and shall: (1) Assist the controller in meeting the controller's obligations under sections 8 to 13, inclusive, of this act taking into account (A) the nature of the processing, (B) the information available to the processor by appropriate technical and organizational measures, and (C) whether such assistance is reasonably practicable and necessary to assist the controller in meeting such obligations; and (2) provide any information that is necessary to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall satisfy the requirements established in subsection (b) of section 42-521 of the general statutes.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 8 to 13, inclusive, of this act.



### ***Substitute Senate Bill No. 3***

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 13 of this act.

Sec. 12. (NEW) (*Effective October 1, 2024*) (a) The provisions of sections 8 to 11, inclusive, and section 13 of this act shall not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time; (3) individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees; (4) national securities association that is registered under 15 USC 78o-3, as amended from time to time; (5) financial institution or data that is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; (6) covered entity or business associate, as defined in 45 CFR 160.103, as amended from time to time; (7) tribal nation government organization; or (8) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended

**Substitute Senate Bill No. 3**

from time to time.

(b) The following information and data is exempt from the provisions of sections 8 to 11, inclusive, and section 13 of this act: (1) Protected health information; (2) patient-identifying information for the purposes of 42 USC 290dd-2, as amended from time to time; (3) identifiable private information for the purposes of the federal policy for the protection of human subjects under 45 CFR 46, as amended from time to time; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, as amended from time to time; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, as amended from time to time, or personal data used or shared in research, as defined in 45 CFR 164.501, as amended from time to time, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq., as amended from time to time; (7) patient safety work products for the purposes of section 19a-127o of the general statutes and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification under HIPAA; (9) information originating from and intermingled so as to be indistinguishable from, or information treated in the same manner as, information that is exempt under this subsection and maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population

### ***Substitute Senate Bill No. 3***

health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 8 to 11, inclusive, and section 13 of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) No provision of this section or sections 8 to 11, inclusive, or section 13 of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry,

### ***Substitute Senate Bill No. 3***

investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) take immediate steps to protect an interest that is essential for the life or physical safety of the minor or another individual, and where the processing cannot be manifestly based on another legal basis; (6) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action; (7) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or processor, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller or processor has implemented reasonable safeguards to mitigate privacy risks associated with research, including, but not limited to, any risks associated with re-identification; (8) assist another controller, processor or third party with any obligation under sections 8 to 11, inclusive, or section 13 of this act; or (9) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the minor whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(d) No obligation imposed on a controller or processor under any

***Substitute Senate Bill No. 3***

provision of sections 8 to 11, inclusive, or section 13 of this act shall be construed to restrict a controller's or processor's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are (A) reasonably aligned with the expectations of a minor or reasonably anticipated based on the minor's existing relationship with the controller or processor, or (B) otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a minor.

(e) No controller or processor shall be required to comply with any provision of sections 8 to 11, inclusive, or section 13 of this act if compliance with such provision would violate an evidentiary privilege under the laws of this state, and no such provision shall be construed to prevent a controller or processor from providing, as part of a privileged communication, any personal data concerning a minor to any other person who is covered by such evidentiary privilege.

(f) No provision of sections 8 to 11, inclusive, or section 13 of this act shall be construed to: (1) Impose any obligation on a controller that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t of the general statutes; or (2) apply to any individual's processing of personal data in the course of such individual's purely personal or household activities.

(g) (1) Any personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (A) Reasonably necessary and proportionate to the purposes listed in this section; and (B) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

**Substitute Senate Bill No. 3**

(2) Any controller that collects, uses or retains data pursuant to subsection (d) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to minors concerning such collection, use or retention of personal data.

(h) If any controller or processor processes personal data pursuant to an exemption established in subsections (a) to (g), inclusive, of this section, such controller or processor bears the burden of demonstrating that such processing qualifies for such exemption and complies with the requirements established in subsection (g) of this section.

Sec. 13. (NEW) (*Effective October 1, 2024*) (a) Any violation of the provisions of sections 8 to 12, inclusive, of this act shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section or sections 8 to 12, inclusive, of this act shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

(b) (1) During the period beginning October 1, 2024, and ending December 31, 2025, if the Attorney General, in the Attorney General's discretion, determines that a controller or processor has violated any provision of sections 8 to 12, inclusive, of this act but may cure such alleged violation, the Attorney General shall provide written notice to such controller or processor, in a form and manner prescribed by the Attorney General and before the Attorney General commences any action to enforce such provision, disclosing such alleged violation and such provision.

(2) (A) Not later than thirty days after a controller or processor

**Substitute Senate Bill No. 3**

receives a notice under subdivision (1) of this subsection, the controller or processor may send a notice to the Attorney General, in a form and manner prescribed by the Attorney General, disclosing that such controller or processor has: (i) Determined that such controller or processor did not commit the alleged violation of sections 8 to 12, inclusive, of this act; or (ii) cured such violation and taken measures that are sufficient to prevent further such violations.

(B) If the Attorney General receives a notice described in subparagraph (A) of this subdivision and determines, in the Attorney General's discretion, that the controller or processor that sent such notice did not commit the alleged violation or has cured such violation and taken the measures described in subparagraph (A)(ii) of this subdivision, such controller or processor shall not be liable for any civil penalty under subsection (a) of this section.

(C) Not later than February 1, 2026, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law. Such report shall disclose: (i) The number of notices the Attorney General has issued pursuant to subdivision (1) of this subsection; (ii) the number of violations that were cured pursuant to subparagraphs (A) and (B) of this subdivision; and (iii) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2026, the Attorney General may, in the Attorney General's discretion, provide to a controller or processor an opportunity to cure any alleged violation of the provisions of sections 8 to 12, inclusive, of this act in the manner described in subdivisions (1) and (2) of subsection (b) of this section. In determining whether to grant the controller or processor an opportunity to cure such alleged violation, the Attorney General may consider: (1) The number of such violations that such controller or processor is alleged to have committed; (2) the

**Substitute Senate Bill No. 3**

size and complexity of such controller or processor; (3) the nature and extent of such controller's or processor's processing activities; (4) whether there exists a substantial likelihood that such alleged violation has caused or will cause public injury; (5) the safety of persons or property; (6) whether such alleged violation was likely caused by a human or technical error; and (7) the sensitivity of the data.

Sec. 14. Section 21a-435 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective January 1, 2024*):

As used in this section, [and] sections 21a-436 to 21a-439, inclusive, as amended by this act, and section 15 of this act:

(1) "Connecticut user" means a user who provides a Connecticut home address or zip code when registering with an online dating operator or a user who is known or determined by an online dating operator or its online dating platform to be in Connecticut at the time of registration;

(2) "Criminal background screening" means a name search for an individual's history of criminal convictions that is conducted by searching an (A) available and regularly updated government public record database that in the aggregate provides national coverage for searching an individual's history of criminal convictions; or (B) a regularly updated database maintained by a private vendor that provides national coverage for searching an individual's history of criminal convictions and sexual offender registries;

(3) "Criminal conviction" means a conviction for a crime in this state, another state, or under federal law;

(4) "Online dating" means the act of using a digital service to initiate relationships with other individuals for the purpose of romance, sex or marriage;



**Substitute Senate Bill No. 3**

(5) "Online dating operator" means a person who operates a software application designed to facilitate online dating;

(6) "Online dating platform" means a digital service designed to allow users to interact through the Internet to participate in online dating; and

(7) "User" means an individual who uses the online dating services of an online dating operator.

Sec. 15. (NEW) (*Effective January 1, 2024*) (a) Each online dating operator that offers services to Connecticut users shall maintain an online safety center, which shall be reasonably designed to provide Connecticut users with resources concerning safe dating. Each online safety center maintained pursuant to this subsection shall provide: (1) An explanation of the online dating operator's reporting mechanism for harmful or unwanted behavior; (2) safety advice for use when communicating online and meeting in person; (3) a link to an Internet web site or a telephone number where a Connecticut user may access resources concerning domestic violence and sexual harassment; and (4) educational information concerning romance scams.

(b) Each online dating operator that offers services to Connecticut users shall adopt a policy for the online dating platform's handling of harassment reports by or between users.

Sec. 16. Section 21a-439 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective January 1, 2024*):

(a) The Department of Consumer Protection may issue fines of not more than twenty-five thousand dollars per violation, accept an offer in compromise, or take other actions permitted by the general statutes or the regulations of Connecticut state agencies if an online dating operator fails to comply with the provisions of sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act.

**Substitute Senate Bill No. 3**

(b) The Commissioner of Consumer Protection, or the commissioner's designee, may conduct investigations and hold hearings on any matter under the provisions of this section, [and] sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act. The commissioner, or the commissioner's designee, may issue subpoenas, administer oaths, compel testimony and order the production of books, records and documents. If any person refuses to appear, to testify or to produce any book, record or document when so ordered, upon application of the commissioner or the commissioner's designee, a judge of the Superior Court may make such order as may be appropriate to aid in the enforcement of this section.

(c) The Attorney General, at the request of the commissioner or the commissioner's designee, may apply in the name of the state to the Superior Court for an order temporarily or permanently restraining and enjoining any person from violating any provision of this section, [and] sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act.

Sec. 17. Section 29-7b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) There shall be within the Department of Emergency Services and Public Protection a Division of Scientific Services. The Commissioner of Emergency Services and Public Protection shall serve as administrative head of such division, and may delegate jurisdiction over the affairs of such division to a deputy commissioner.

(b) The Division of Scientific Services shall provide technical assistance to law enforcement agencies in the various areas of scientific investigation. The division shall maintain facilities and services for the examination and analysis of evidentiary materials in areas including, but not limited to, chemistry, arson, firearms, questioned documents, microscopy, serology, toxicology, trace evidence, latent fingerprints,

**Substitute Senate Bill No. 3**

impressions and other similar technology. The facilities, services and personnel of the division shall be available, without charge, to the Office of the Chief Medical Examiner and all duly constituted prosecuting, police and investigating agencies of the state.

(c) The Division of Scientific Services: (1) May investigate any physical evidence or evidentiary material related to a crime upon the request of any federal, state or local agency, (2) may conduct or assist in the scientific field investigation at the scene of a crime and provide other technical assistance and training in the various fields of scientific criminal investigation upon request, (3) shall assure the safe custody of evidence during examination, (4) shall forward a written report of the results of an examination of evidence to the agency submitting such evidence, (5) shall render expert court testimony when requested, and (6) shall conduct ongoing research in the areas of the forensic sciences. The Commissioner of Emergency Services and Public Protection or a director designated by the commissioner shall be in charge of the Division of Scientific Services operations and shall establish and maintain a system of case priorities and a procedure for submission of evidence and evidentiary security. The director of the Division of Scientific Services shall be in the unclassified service and shall serve at the pleasure of the commissioner.

(d) In accordance with the provisions of sections 4-38d, 4-38e and 4-39, all powers and duties of the Department of Public Health under the provisions of sections 14-227a, 14-227c, 15-140u and 21a-283 shall be transferred to the Division of Scientific Services within the Department of Emergency Services and Public Protection.

(e) There is established within the Division of Scientific Services the Connecticut Internet Crimes Against Children Task Force, which shall consist of affiliate law enforcement agencies in the state. The task force shall use state and federal moneys appropriated to it in a manner that is consistent with the duties prescribed in 34 USC 21114.

***Substitute Senate Bill No. 3***

Approved June 26, 2023

7

CERTIFICATION OF ENROLLMENT  
**ENGROSSED SUBSTITUTE HOUSE BILL 1155**

68th Legislature  
2023 Regular Session

Passed by the House April 17, 2023  
Yeas 57 Nays 40

---

**Speaker of the House of  
Representatives**

Passed by the Senate April 5, 2023  
Yeas 27 Nays 21

---

**President of the Senate**

Approved

---

**Governor of the State of Washington**

CERTIFICATE

I, Bernard Dean, Chief Clerk of the House of Representatives of the State of Washington, do hereby certify that the attached is **ENGROSSED SUBSTITUTE HOUSE BILL 1155** as passed by the House of Representatives and the Senate on the dates hereon set forth.

---

**Chief Clerk**

FILED

**Secretary of State  
State of Washington**

---

**ENGROSSED SUBSTITUTE HOUSE BILL 1155**

---

AS AMENDED BY THE SENATE

Passed Legislature - 2023 Regular Session

**State of Washington                      68th Legislature                      2023 Regular Session**

**By** House Civil Rights & Judiciary (originally sponsored by Representatives Slatter, Street, Reed, Ryu, Berg, Alvarado, Taylor, Bateman, Ramel, Senn, Goodman, Fitzgibbon, Macri, Simmons, Reeves, Lekanoff, Orwall, Duerr, Thai, Gregerson, Wylie, Ortiz-Self, Stonier, Pollet, Riccelli, Donaghy, Fosse, and Ormsby; by request of Attorney General)

READ FIRST TIME 02/07/23.

1            AN ACT Relating to the collection, sharing, and selling of  
2 consumer health data; adding a new section to chapter 44.28 RCW;  
3 adding a new chapter to Title 19 RCW; and providing an expiration  
4 date.

5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

6            NEW SECTION.    **Sec. 1.**    This act may be known and cited as the  
7 Washington my health my data act.

8            NEW SECTION.    **Sec. 2.**    (1) The legislature finds that the people  
9 of Washington regard their privacy as a fundamental right and an  
10 essential element of their individual freedom. Washington's  
11 Constitution explicitly provides the right to privacy. Fundamental  
12 privacy rights have long been and continue to be integral to  
13 protecting Washingtonians and to safeguarding our democratic  
14 republic.

15            (2) Information related to an individual's health conditions or  
16 attempts to obtain health care services is among the most personal  
17 and sensitive categories of data collected. Washingtonians expect  
18 that their health data is protected under laws like the health  
19 information portability and accountability act (HIPAA). However,  
20 HIPAA only covers health data collected by specific health care

1 entities, including most health care providers. Health data collected  
2 by noncovered entities, including certain apps and websites, are not  
3 afforded the same protections. This act works to close the gap  
4 between consumer knowledge and industry practice by providing  
5 stronger privacy protections for all Washington consumers' health  
6 data.

7 (3) With this act, the legislature intends to provide heightened  
8 protections for Washingtonian's health data by: Requiring additional  
9 disclosures and consumer consent regarding the collection, sharing,  
10 and use of such information; empowering consumers with the right to  
11 have their health data deleted; prohibiting the selling of consumer  
12 health data without valid authorization signed by the consumer; and  
13 making it unlawful to utilize a geofence around a facility that  
14 provides health care services.

15 NEW SECTION. **Sec. 3.** The definitions in this section apply  
16 throughout this chapter unless the context clearly requires  
17 otherwise.

18 (1) "Abortion" means the termination of a pregnancy for purposes  
19 other than producing a live birth.

20 (2) "Affiliate" means a legal entity that shares common branding  
21 with another legal entity and controls, is controlled by, or is under  
22 common control with another legal entity. For the purposes of this  
23 definition, "control" or "controlled" means:

24 (a) Ownership of, or the power to vote, more than 50 percent of  
25 the outstanding shares of any class of voting security of a company;

26 (b) Control in any manner over the election of a majority of the  
27 directors or of individuals exercising similar functions; or

28 (c) The power to exercise controlling influence over the  
29 management of a company.

30 (3) "Authenticate" means to use reasonable means to determine  
31 that a request to exercise any of the rights afforded in this chapter  
32 is being made by, or on behalf of, the consumer who is entitled to  
33 exercise such consumer rights with respect to the consumer health  
34 data at issue.

35 (4) "Biometric data" means data that is generated from the  
36 measurement or technological processing of an individual's  
37 physiological, biological, or behavioral characteristics and that  
38 identifies a consumer, whether individually or in combination with  
39 other data. Biometric data includes, but is not limited to:



1 (a) Imagery of the iris, retina, fingerprint, face, hand, palm,  
2 vein patterns, and voice recordings, from which an identifier  
3 template can be extracted; or

4 (b) Keystroke patterns or rhythms and gait patterns or rhythms  
5 that contain identifying information.

6 (5) "Collect" means to buy, rent, access, retain, receive,  
7 acquire, infer, derive, or otherwise process consumer health data in  
8 any manner.

9 (6) (a) "Consent" means a clear affirmative act that signifies a  
10 consumer's freely given, specific, informed, opt-in, voluntary, and  
11 unambiguous agreement, which may include written consent provided by  
12 electronic means.

13 (b) "Consent" may not be obtained by:

14 (i) A consumer's acceptance of a general or broad terms of use  
15 agreement or a similar document that contains descriptions of  
16 personal data processing along with other unrelated information;

17 (ii) A consumer hovering over, muting, pausing, or closing a  
18 given piece of content; or

19 (iii) A consumer's agreement obtained through the use of  
20 deceptive designs.

21 (7) "Consumer" means (a) a natural person who is a Washington  
22 resident; or (b) a natural person whose consumer health data is  
23 collected in Washington. "Consumer" means a natural person who acts  
24 only in an individual or household context, however identified,  
25 including by any unique identifier. "Consumer" does not include an  
26 individual acting in an employment context.

27 (8) (a) "Consumer health data" means personal information that is  
28 linked or reasonably linkable to a consumer and that identifies the  
29 consumer's past, present, or future physical or mental health status.

30 (b) For the purposes of this definition, physical or mental  
31 health status includes, but is not limited to:

32 (i) Individual health conditions, treatment, diseases, or  
33 diagnosis;

34 (ii) Social, psychological, behavioral, and medical  
35 interventions;

36 (iii) Health-related surgeries or procedures;

37 (iv) Use or purchase of prescribed medication;

38 (v) Bodily functions, vital signs, symptoms, or measurements of  
39 the information described in this subsection (8) (b);

40 (vi) Diagnoses or diagnostic testing, treatment, or medication;

1 (vii) Gender-affirming care information;  
2 (viii) Reproductive or sexual health information;  
3 (ix) Biometric data;  
4 (x) Genetic data;  
5 (xi) Precise location information that could reasonably indicate  
6 a consumer's attempt to acquire or receive health services or  
7 supplies;  
8 (xii) Data that identifies a consumer seeking health care  
9 services; or  
10 (xiii) Any information that a regulated entity or a small  
11 business, or their respective processor, processes to associate or  
12 identify a consumer with the data described in (b)(i) through (xii)  
13 of this subsection that is derived or extrapolated from nonhealth  
14 information (such as proxy, derivative, inferred, or emergent data by  
15 any means, including algorithms or machine learning).

16 (c) "Consumer health data" does not include personal information  
17 that is used to engage in public or peer-reviewed scientific,  
18 historical, or statistical research in the public interest that  
19 adheres to all other applicable ethics and privacy laws and is  
20 approved, monitored, and governed by an institutional review board,  
21 human subjects research ethics review board, or a similar independent  
22 oversight entity that determines that the regulated entity or the  
23 small business has implemented reasonable safeguards to mitigate  
24 privacy risks associated with research, including any risks  
25 associated with reidentification.

26 (9) "Deceptive design" means a user interface designed or  
27 manipulated with the effect of subverting or impairing user autonomy,  
28 decision making, or choice.

29 (10) "Deidentified data" means data that cannot reasonably be  
30 used to infer information about, or otherwise be linked to, an  
31 identified or identifiable consumer, or a device linked to such  
32 consumer, if the regulated entity or the small business that  
33 possesses such data (a) takes reasonable measures to ensure that such  
34 data cannot be associated with a consumer; (b) publicly commits to  
35 process such data only in a deidentified fashion and not attempt to  
36 reidentify such data; and (c) contractually obligates any recipients  
37 of such data to satisfy the criteria set forth in this subsection  
38 (10).

39 (11) "Gender-affirming care information" means personal  
40 information relating to seeking or obtaining past, present, or future

1 gender-affirming care services. "Gender-affirming care information"  
2 includes, but is not limited to:

3 (a) Precise location information that could reasonably indicate a  
4 consumer's attempt to acquire or receive gender-affirming care  
5 services;

6 (b) Efforts to research or obtain gender-affirming care services;  
7 or

8 (c) Any gender-affirming care information that is derived,  
9 extrapolated, or inferred, including from nonhealth information, such  
10 as proxy, derivative, inferred, emergent, or algorithmic data.

11 (12) "Gender-affirming care services" means health services or  
12 products that support and affirm an individual's gender identity  
13 including, but not limited to, social, psychological, behavioral,  
14 cosmetic, medical, or surgical interventions. "Gender-affirming care  
15 services" includes, but is not limited to, treatments for gender  
16 dysphoria, gender-affirming hormone therapy, and gender-affirming  
17 surgical procedures.

18 (13) "Genetic data" means any data, regardless of its format,  
19 that concerns a consumer's genetic characteristics. "Genetic data"  
20 includes, but is not limited to:

21 (a) Raw sequence data that result from the sequencing of a  
22 consumer's complete extracted deoxyribonucleic acid (DNA) or a  
23 portion of the extracted DNA;

24 (b) Genotypic and phenotypic information that results from  
25 analyzing the raw sequence data; and

26 (c) Self-reported health data that a consumer submits to a  
27 regulated entity or a small business and that is analyzed in  
28 connection with consumer's raw sequence data.

29 (14) "Geofence" means technology that uses global positioning  
30 coordinates, cell tower connectivity, cellular data, radio frequency  
31 identification, Wifi data, and/or any other form of spatial or  
32 location detection to establish a virtual boundary around a specific  
33 physical location, or to locate a consumer within a virtual boundary.  
34 For purposes of this definition, "geofence" means a virtual boundary  
35 that is 2,000 feet or less from the perimeter of the physical  
36 location.

37 (15) "Health care services" means any service provided to a  
38 person to assess, measure, improve, or learn about a person's mental  
39 or physical health, including but not limited to:

40 (a) Individual health conditions, status, diseases, or diagnoses;

- 1 (b) Social, psychological, behavioral, and medical interventions;
- 2 (c) Health-related surgeries or procedures;
- 3 (d) Use or purchase of medication;
- 4 (e) Bodily functions, vital signs, symptoms, or measurements of
- 5 the information described in this subsection;
- 6 (f) Diagnoses or diagnostic testing, treatment, or medication;
- 7 (g) Reproductive health care services; or
- 8 (h) Gender-affirming care services.

9 (16) "Homepage" means the introductory page of an internet  
10 website and any internet webpage where personal information is  
11 collected. In the case of an online service, such as a mobile  
12 application, homepage means the application's platform page or  
13 download page, and a link within the application, such as from the  
14 application configuration, "about," "information," or settings page.

15 (17) "Person" means, where applicable, natural persons,  
16 corporations, trusts, unincorporated associations, and partnerships.  
17 "Person" does not include government agencies, tribal nations, or  
18 contracted service providers when processing consumer health data on  
19 behalf of a government agency.

20 (18)(a) "Personal information" means information that identifies  
21 or is reasonably capable of being associated or linked, directly or  
22 indirectly, with a particular consumer. "Personal information"  
23 includes, but is not limited to, data associated with a persistent  
24 unique identifier, such as a cookie ID, an IP address, a device  
25 identifier, or any other form of persistent unique identifier.

26 (b) "Personal information" does not include publicly available  
27 information.

28 (c) "Personal information" does not include deidentified data.

29 (19) "Precise location information" means information derived  
30 from technology including, but not limited to, global positioning  
31 system level latitude and longitude coordinates or other mechanisms,  
32 that directly identifies the specific location of an individual with  
33 precision and accuracy within a radius of 1,750 feet. "Precise  
34 location information" does not include the content of communications,  
35 or any data generated by or connected to advanced utility metering  
36 infrastructure systems or equipment for use by a utility.

37 (20) "Process" or "processing" means any operation or set of  
38 operations performed on consumer health data.

39 (21) "Processor" means a person that processes consumer health  
40 data on behalf of a regulated entity or a small business.

1 (22) "Publicly available information" means information that (a)  
2 is lawfully made available through federal, state, or municipal  
3 government records or widely distributed media, and (b) a regulated  
4 entity or a small business has a reasonable basis to believe a  
5 consumer has lawfully made available to the general public. "Publicly  
6 available information" does not include any biometric data collected  
7 about a consumer by a business without the consumer's consent.

8 (23) "Regulated entity" means any legal entity that: (a) Conducts  
9 business in Washington, or produces or provides products or services  
10 that are targeted to consumers in Washington; and (b) alone or  
11 jointly with others, determines the purpose and means of collecting,  
12 processing, sharing, or selling of consumer health data. "Regulated  
13 entity" does not mean government agencies, tribal nations, or  
14 contracted service providers when processing consumer health data on  
15 behalf of the government agency.

16 (24) "Reproductive or sexual health information" means personal  
17 information relating to seeking or obtaining past, present, or future  
18 reproductive or sexual health services. "Reproductive or sexual  
19 health information" includes, but is not limited to:

20 (a) Precise location information that could reasonably indicate a  
21 consumer's attempt to acquire or receive reproductive or sexual  
22 health services;

23 (b) Efforts to research or obtain reproductive or sexual health  
24 services; or

25 (c) Any reproductive or sexual health information that is  
26 derived, extrapolated, or inferred, including from nonhealth  
27 information (such as proxy, derivative, inferred, emergent, or  
28 algorithmic data).

29 (25) "Reproductive or sexual health services" means health  
30 services or products that support or relate to a consumer's  
31 reproductive system or sexual well-being, including but not limited  
32 to:

33 (a) Individual health conditions, status, diseases, or diagnoses;

34 (b) Social, psychological, behavioral, and medical interventions;

35 (c) Health-related surgeries or procedures including, but not  
36 limited to, abortions;

37 (d) Use or purchase of medication including, but not limited to,  
38 medications for the purposes of abortion;

39 (e) Bodily functions, vital signs, symptoms, or measurements of  
40 the information described in this subsection;

1 (f) Diagnoses or diagnostic testing, treatment, or medication;  
2 and

3 (g) Medical or nonmedical services related to and provided in  
4 conjunction with an abortion, including but not limited to associated  
5 diagnostics, counseling, supplies, and follow-up services.

6 (26)(a) "Sell" or "sale" means the exchange of consumer health  
7 data for monetary or other valuable consideration.

8 (b) "Sell" or "sale" does not include the exchange of consumer  
9 health data for monetary or other valuable consideration:

10 (i) To a third party as an asset that is part of a merger,  
11 acquisition, bankruptcy, or other transaction in which the third  
12 party assumes control of all or part of the regulated entity's or the  
13 small business's assets that complies with the requirements and  
14 obligations in this chapter; or

15 (ii) By a regulated entity or a small business to a processor  
16 when such exchange is consistent with the purpose for which the  
17 consumer health data was collected and disclosed to the consumer.

18 (27)(a) "Share" or "sharing" means to release, disclose,  
19 disseminate, divulge, make available, provide access to, license, or  
20 otherwise communicate orally, in writing, or by electronic or other  
21 means, consumer health data by a regulated entity or a small business  
22 to a third party or affiliate.

23 (b) The term "share" or "sharing" does not include:

24 (i) The disclosure of consumer health data by a regulated entity  
25 or a small business to a processor when such sharing is to provide  
26 goods or services in a manner consistent with the purpose for which  
27 the consumer health data was collected and disclosed to the consumer;

28 (ii) The disclosure of consumer health data to a third party with  
29 whom the consumer has a direct relationship when: (A) The disclosure  
30 is for purposes of providing a product or service requested by the  
31 consumer; (B) the regulated entity or the small business maintains  
32 control and ownership of the data; and (C) the third party uses the  
33 consumer health data only at direction from the regulated entity or  
34 the small business and consistent with the purpose for which it was  
35 collected and consented to by the consumer; or

36 (iii) The disclosure or transfer of personal data to a third  
37 party as an asset that is part of a merger, acquisition, bankruptcy,  
38 or other transaction in which the third party assumes control of all  
39 or part of the regulated entity's or the small business's assets and  
40 complies with the requirements and obligations in this chapter.

1 (28) "Small business" means a regulated entity that satisfies one  
2 or both of the following thresholds:

3 (a) Collects, processes, sells, or shares consumer health data of  
4 fewer than 100,000 consumers during a calendar year; or

5 (b) Derives less than 50 percent of gross revenue from the  
6 collection, processing, selling, or sharing of consumer health data,  
7 and controls, processes, sells, or shares consumer health data of  
8 fewer than 25,000 consumers.

9 (29) "Third party" means an entity other than a consumer,  
10 regulated entity, processor, small business, or affiliate of the  
11 regulated entity or the small business.

12 NEW SECTION. **Sec. 4.** (1)(a) Except as provided in subsection  
13 (2) of this section, beginning March 31, 2024, a regulated entity and  
14 a small business shall maintain a consumer health data privacy policy  
15 that clearly and conspicuously discloses:

16 (i) The categories of consumer health data collected and the  
17 purpose for which the data is collected, including how the data will  
18 be used;

19 (ii) The categories of sources from which the consumer health  
20 data is collected;

21 (iii) The categories of consumer health data that is shared;

22 (iv) A list of the categories of third parties and specific  
23 affiliates with whom the regulated entity or the small business  
24 shares the consumer health data; and

25 (v) How a consumer can exercise the rights provided in section 6  
26 of this act.

27 (b) A regulated entity and a small business shall prominently  
28 publish a link to its consumer health data privacy policy on its  
29 homepage.

30 (c) A regulated entity or a small business may not collect, use,  
31 or share additional categories of consumer health data not disclosed  
32 in the consumer health data privacy policy without first disclosing  
33 the additional categories and obtaining the consumer's affirmative  
34 consent prior to the collection, use, or sharing of such consumer  
35 health data.

36 (d) A regulated entity or a small business may not collect, use,  
37 or share consumer health data for additional purposes not disclosed  
38 in the consumer health data privacy policy without first disclosing  
39 the additional purposes and obtaining the consumer's affirmative

1 consent prior to the collection, use, or sharing of such consumer  
2 health data.

3 (e) It is a violation of this chapter for a regulated entity or a  
4 small business to contract with a processor to process consumer  
5 health data in a manner that is inconsistent with the regulated  
6 entity's or the small business's consumer health data privacy policy.

7 (2) A small business must comply with this section beginning June  
8 30, 2024.

9 NEW SECTION. **Sec. 5.** (1)(a) Except as provided in subsection  
10 (2) of this section, beginning March 31, 2024, a regulated entity or  
11 a small business may not collect any consumer health data except:

12 (i) With consent from the consumer for such collection for a  
13 specified purpose; or

14 (ii) To the extent necessary to provide a product or service that  
15 the consumer to whom such consumer health data relates has requested  
16 from such regulated entity or small business.

17 (b) A regulated entity or a small business may not share any  
18 consumer health data except:

19 (i) With consent from the consumer for such sharing that is  
20 separate and distinct from the consent obtained to collect consumer  
21 health data; or

22 (ii) To the extent necessary to provide a product or service that  
23 the consumer to whom such consumer health data relates has requested  
24 from such regulated entity or small business.

25 (c) Consent required under this section must be obtained prior to  
26 the collection or sharing, as applicable, of any consumer health  
27 data, and the request for consent must clearly and conspicuously  
28 disclose: (i) The categories of consumer health data collected or  
29 shared; (ii) the purpose of the collection or sharing of the consumer  
30 health data, including the specific ways in which it will be used;  
31 (iii) the categories of entities with whom the consumer health data  
32 is shared; and (iv) how the consumer can withdraw consent from future  
33 collection or sharing of the consumer's health data.

34 (d) A regulated entity or a small business may not unlawfully  
35 discriminate against a consumer for exercising any rights included in  
36 this chapter.

37 (2) A small business must comply with this section beginning June  
38 30, 2024.



1        NEW SECTION.    **Sec. 6.**    (1)(a) Except as provided in subsection  
2 (2) of this section, beginning March 31, 2024, a consumer has the  
3 right to confirm whether a regulated entity or a small business is  
4 collecting, sharing, or selling consumer health data concerning the  
5 consumer and to access such data, including a list of all third  
6 parties and affiliates with whom the regulated entity or the small  
7 business has shared or sold the consumer health data and an active  
8 email address or other online mechanism that the consumer may use to  
9 contact these third parties.

10        (b) A consumer has the right to withdraw consent from the  
11 regulated entity's or the small business's collection and sharing of  
12 consumer health data concerning the consumer.

13        (c) A consumer has the right to have consumer health data  
14 concerning the consumer deleted and may exercise that right by  
15 informing the regulated entity or the small business of the  
16 consumer's request for deletion.

17        (i) A regulated entity or a small business that receives a  
18 consumer's request to delete any consumer health data concerning the  
19 consumer shall:

20        (A) Delete the consumer health data from its records, including  
21 from all parts of the regulated entity's or the small business's  
22 network, including archived or backup systems pursuant to (c)(iii) of  
23 this subsection; and

24        (B) Notify all affiliates, processors, contractors, and other  
25 third parties with whom the regulated entity or the small business  
26 has shared consumer health data of the deletion request.

27        (ii) All affiliates, processors, contractors, and other third  
28 parties that receive notice of a consumer's deletion request shall  
29 honor the consumer's deletion request and delete the consumer health  
30 data from its records, subject to the same requirements of this  
31 chapter.

32        (iii) If consumer health data that a consumer requests to be  
33 deleted is stored on archived or backup systems, then the request for  
34 deletion may be delayed to enable restoration of the archived or  
35 backup systems and such delay may not exceed six months from  
36 authenticating the deletion request.

37        (d) A consumer may exercise the rights set forth in this chapter  
38 by submitting a request, at any time, to a regulated entity or a  
39 small business. Such a request may be made by a secure and reliable  
40 means established by the regulated entity or the small business and

1 described in its consumer health data privacy policy. The method must  
2 take into account the ways in which consumers normally interact with  
3 the regulated entity or the small business, the need for secure and  
4 reliable communication of such requests, and the ability of the  
5 regulated entity or the small business to authenticate the identity  
6 of the consumer making the request. A regulated entity or a small  
7 business may not require a consumer to create a new account in order  
8 to exercise consumer rights pursuant to this chapter but may require  
9 a consumer to use an existing account.

10 (e) If a regulated entity or a small business is unable to  
11 authenticate the request using commercially reasonable efforts, the  
12 regulated entity or the small business is not required to comply with  
13 a request to initiate an action under this section and may request  
14 that the consumer provide additional information reasonably necessary  
15 to authenticate the consumer and the consumer's request.

16 (f) Information provided in response to a consumer request must  
17 be provided by a regulated entity and a small business free of  
18 charge, up to twice annually per consumer. If requests from a  
19 consumer are manifestly unfounded, excessive, or repetitive, the  
20 regulated entity or the small business may charge the consumer a  
21 reasonable fee to cover the administrative costs of complying with  
22 the request or decline to act on the request. The regulated entity  
23 and the small business bear the burden of demonstrating the  
24 manifestly unfounded, excessive, or repetitive nature of the request.

25 (g) A regulated entity and a small business shall comply with the  
26 consumer's requests under subsection (1)(a) through (c) of this  
27 section without undue delay, but in all cases within 45 days of  
28 receipt of the request submitted pursuant to the methods described in  
29 this section. A regulated entity and a small business must promptly  
30 take steps to authenticate a consumer request but this does not  
31 extend the regulated entity's and the small business's duty to comply  
32 with the consumer's request within 45 days of receipt of the  
33 consumer's request. The response period may be extended once by 45  
34 additional days when reasonably necessary, taking into account the  
35 complexity and number of the consumer's requests, so long as the  
36 regulated entity or the small business informs the consumer of any  
37 such extension within the initial 45-day response period, together  
38 with the reason for the extension.

39 (h) A regulated entity and a small business shall establish a  
40 process for a consumer to appeal the regulated entity's or the small

1 business's refusal to take action on a request within a reasonable  
2 period of time after the consumer's receipt of the decision. The  
3 appeal process must be conspicuously available and similar to the  
4 process for submitting requests to initiate action pursuant to this  
5 section. Within 45 days of receipt of an appeal, a regulated entity  
6 or a small business shall inform the consumer in writing of any  
7 action taken or not taken in response to the appeal, including a  
8 written explanation of the reasons for the decisions. If the appeal  
9 is denied, the regulated entity or the small business shall also  
10 provide the consumer with an online mechanism, if available, or other  
11 method through which the consumer may contact the attorney general to  
12 submit a complaint.

13 (2) A small business must comply with this section beginning June  
14 30, 2024.

15 NEW SECTION. **Sec. 7.** (1) Except as provided in subsection (2)  
16 of this section, beginning March 31, 2024, a regulated entity and a  
17 small business shall:

18 (a) Restrict access to consumer health data by the employees,  
19 processors, and contractors of such regulated entity or small  
20 business to only those employees, processors, and contractors for  
21 which access is necessary to further the purposes for which the  
22 consumer provided consent or where necessary to provide a product or  
23 service that the consumer to whom such consumer health data relates  
24 has requested from such regulated entity or small business; and

25 (b) Establish, implement, and maintain administrative, technical,  
26 and physical data security practices that, at a minimum, satisfy  
27 reasonable standard of care within the regulated entity's or the  
28 small business's industry to protect the confidentiality, integrity,  
29 and accessibility of consumer health data appropriate to the volume  
30 and nature of the consumer health data at issue.

31 (2) A small business must comply with this section beginning June  
32 30, 2024.

33 NEW SECTION. **Sec. 8.** (1)(a)(i) Except as provided in subsection  
34 (2) of this section, beginning March 31, 2024, a processor may  
35 process consumer health data only pursuant to a binding contract  
36 between the processor and the regulated entity or the small business  
37 that sets forth the processing instructions and limit the actions the

1 processor may take with respect to the consumer health data it  
2 processes on behalf of the regulated entity or the small business.

3 (ii) A processor may process consumer health data only in a  
4 manner that is consistent with the binding instructions set forth in  
5 the contract with the regulated entity or the small business.

6 (b) A processor shall assist the regulated entity or the small  
7 business by appropriate technical and organizational measures,  
8 insofar as this is possible, in fulfilling the regulated entity's and  
9 the small business's obligations under this chapter.

10 (c) If a processor fails to adhere to the regulated entity's or  
11 the small business's instructions or processes consumer health data  
12 in a manner that is outside the scope of the processor's contract  
13 with the regulated entity or the small business, the processor is  
14 considered a regulated entity or a small business with regard to such  
15 data and is subject to all the requirements of this chapter with  
16 regard to such data.

17 (2) A small business must comply with this section beginning June  
18 30, 2024.

19 NEW SECTION. **Sec. 9.** (1) Except as provided in subsection (6)  
20 of this section, beginning March 31, 2024, it is unlawful for any  
21 person to sell or offer to sell consumer health data concerning a  
22 consumer without first obtaining valid authorization from the  
23 consumer. The sale of consumer health data must be consistent with  
24 the valid authorization signed by the consumer. This authorization  
25 must be separate and distinct from the consent obtained to collect or  
26 share consumer health data, as required under section 5 of this act.

27 (2) A valid authorization to sell consumer health data is a  
28 document consistent with this section and must be written in plain  
29 language. The valid authorization to sell consumer health data must  
30 contain the following:

31 (a) The specific consumer health data concerning the consumer  
32 that the person intends to sell;

33 (b) The name and contact information of the person collecting and  
34 selling the consumer health data;

35 (c) The name and contact information of the person purchasing the  
36 consumer health data from the seller identified in (b) of this  
37 subsection;

1 (d) A description of the purpose for the sale, including how the  
2 consumer health data will be gathered and how it will be used by the  
3 purchaser identified in (c) of this subsection when sold;

4 (e) A statement that the provision of goods or services may not  
5 be conditioned on the consumer signing the valid authorization;

6 (f) A statement that the consumer has a right to revoke the valid  
7 authorization at any time and a description on how to submit a  
8 revocation of the valid authorization;

9 (g) A statement that the consumer health data sold pursuant to  
10 the valid authorization may be subject to redisclosure by the  
11 purchaser and may no longer be protected by this section;

12 (h) An expiration date for the valid authorization that expires  
13 one year from when the consumer signs the valid authorization; and

14 (i) The signature of the consumer and date.

15 (3) An authorization is not valid if the document has any of the  
16 following defects:

17 (a) The expiration date has passed;

18 (b) The authorization does not contain all the information  
19 required under this section;

20 (c) The authorization has been revoked by the consumer;

21 (d) The authorization has been combined with other documents to  
22 create a compound authorization; or

23 (e) The provision of goods or services is conditioned on the  
24 consumer signing the authorization.

25 (4) A copy of the signed valid authorization must be provided to  
26 the consumer.

27 (5) The seller and purchaser of consumer health data must retain  
28 a copy of all valid authorizations for sale of consumer health data  
29 for six years from the date of its signature or the date when it was  
30 last in effect, whichever is later.

31 (6) A small business must comply with this section beginning June  
32 30, 2024.

33 NEW SECTION. **Sec. 10.** It is unlawful for any person to  
34 implement a geofence around an entity that provides in-person health  
35 care services where such geofence is used to: (1) Identify or track  
36 consumers seeking health care services; (2) collect consumer health  
37 data from consumers; or (3) send notifications, messages, or  
38 advertisements to consumers related to their consumer health data or  
39 health care services.

1        NEW SECTION.    **Sec. 11.**    The legislature finds that the practices  
2 covered by this chapter are matters vitally affecting the public  
3 interest for the purpose of applying the consumer protection act,  
4 chapter 19.86 RCW. A violation of this chapter is not reasonable in  
5 relation to the development and preservation of business, and is an  
6 unfair or deceptive act in trade or commerce and an unfair method of  
7 competition for the purpose of applying the consumer protection act,  
8 chapter 19.86 RCW.

9        NEW SECTION.    **Sec. 12.**    (1) This chapter does not apply to:

10        (a) Information that meets the definition of:

11        (i) Protected health information for purposes of the federal  
12 health insurance portability and accountability act of 1996 and  
13 related regulations;

14        (ii) Health care information collected, used, or disclosed in  
15 accordance with chapter 70.02 RCW;

16        (iii) Patient identifying information collected, used, or  
17 disclosed in accordance with 42 C.F.R. Part 2, established pursuant  
18 to 42 U.S.C. Sec. 290dd-2;

19        (iv) Identifiable private information for purposes of the federal  
20 policy for the protection of human subjects, 45 C.F.R. Part 46;  
21 identifiable private information that is otherwise information  
22 collected as part of human subjects research pursuant to the good  
23 clinical practice guidelines issued by the international council for  
24 harmonization; the protection of human subjects under 21 C.F.R. Parts  
25 50 and 56; or personal data used or shared in research conducted in  
26 accordance with one or more of the requirements set forth in this  
27 subsection;

28        (v) Information and documents created specifically for, and  
29 collected and maintained by:

30        (A) A quality improvement committee for purposes of RCW  
31 43.70.510, 70.230.080, or 70.41.200;

32        (B) A peer review committee for purposes of RCW 4.24.250;

33        (C) A quality assurance committee for purposes of RCW 74.42.640  
34 or 18.20.390;

35        (D) A hospital, as defined in RCW 43.70.056, for reporting of  
36 health care-associated infections for purposes of RCW 43.70.056, a  
37 notification of an incident for purposes of RCW 70.56.040(5), or  
38 reports regarding adverse events for purposes of RCW 70.56.020(2)(b);  
39 or

1 (E) A manufacturer, as defined in 21 C.F.R. Sec. 820.3(o), when  
2 collected, used, or disclosed for purposes specified in chapter 70.02  
3 RCW;

4 (vi) Information and documents created for purposes of the  
5 federal health care quality improvement act of 1986, and related  
6 regulations;

7 (vii) Patient safety work product for purposes of 42 C.F.R. Part  
8 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

9 (viii) Information that is (A) deidentified in accordance with  
10 the requirements for deidentification set forth in 45 C.F.R. Part  
11 164, and (B) derived from any of the health care-related information  
12 listed in this subsection (1)(a)(viii);

13 (b) Information originating from, and intermingled to be  
14 indistinguishable with, information under (a) of this subsection that  
15 is maintained by:

16 (i) A covered entity or business associate as defined by the  
17 health insurance portability and accountability act of 1996 and  
18 related regulations;

19 (ii) A health care facility or health care provider as defined in  
20 RCW 70.02.010; or

21 (iii) A program or a qualified service organization as defined by  
22 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

23 (c) Information used only for public health activities and  
24 purposes as described in 45 C.F.R. Sec. 164.512 or that is part of a  
25 limited data set, as defined, and is used, disclosed, and maintained  
26 in the manner required, by 45 C.F.R. Sec. 164.514; or

27 (d) Identifiable data collected, used, or disclosed in accordance  
28 with chapter 43.371 RCW or RCW 69.43.165.

29 (2) Personal information that is governed by and collected, used,  
30 or disclosed pursuant to the following regulations, parts, titles, or  
31 acts, is exempt from this chapter: (a) The Gramm-Leach-Bliley act (15  
32 U.S.C. 6801 et seq.) and implementing regulations; (b) part C of  
33 Title XI of the social security act (42 U.S.C. 1320d et seq.); (c)  
34 the fair credit reporting act (15 U.S.C. 1681 et seq.); (d) the  
35 family educational rights and privacy act (20 U.S.C. 1232g; Part 99  
36 of Title 34, C.F.R.); (e) the Washington health benefit exchange and  
37 applicable statutes and regulations, including 45 C.F.R. Sec. 155.260  
38 and chapter 43.71 RCW; or (f) privacy rules adopted by the office of  
39 the insurance commissioner pursuant to chapter 48.02 or 48.43 RCW.

1 (3) The obligations imposed on regulated entities, small  
2 businesses, and processors under this chapter does not restrict a  
3 regulated entity's, small business's, or processor's ability for  
4 collection, use, or disclosure of consumer health data to prevent,  
5 detect, protect against, or respond to security incidents, identity  
6 theft, fraud, harassment, malicious or deceptive activities, or any  
7 activity that is illegal under Washington state law or federal law;  
8 preserve the integrity or security of systems; or investigate,  
9 report, or prosecute those responsible for any such action that is  
10 illegal under Washington state law or federal law.

11 (4) If a regulated entity, small business, or processor processes  
12 consumer health data pursuant to subsection (3) of this section, such  
13 entity bears the burden of demonstrating that such processing  
14 qualifies for the exemption and complies with the requirements of  
15 this section.

16 NEW SECTION. **Sec. 13.** A new section is added to chapter 44.28  
17 RCW to read as follows:

18 (1) The joint committee must review enforcement actions, as  
19 authorized in section 11 of this act, brought by the attorney general  
20 and consumers to enforce violations of this act.

21 (2) The report must include, at a minimum:

22 (a) The number of enforcement actions reported by the attorney  
23 general, a consumer, a regulated entity, or a small business that  
24 resulted in a settlement, including the average settlement amount;

25 (b) The number of complaints reported, including categories of  
26 complaints and the number of complaints for each category, reported  
27 by the attorney general, a consumer, a regulated entity, or a small  
28 business;

29 (c) The number of enforcement actions brought by the attorney  
30 general and consumers, including the categories of violations and the  
31 number of violations per category;

32 (e) The number of civil actions where a judge determined the  
33 position of the nonprevailing party was frivolous, if any;

34 (f) The types of resources, including associated costs, expended  
35 by the attorney general, a consumer, a regulated entity, or a small  
36 business for enforcement actions; and

37 (g) Recommendations for potential changes to enforcement  
38 provisions of this act.



1 (3) The office of the attorney general shall provide the joint  
2 committee any data within their purview that the joint committee  
3 considers necessary to conduct the review.

4 (4) The joint committee shall submit a report of its findings and  
5 recommendations to the governor and the appropriate committees of the  
6 legislature by September 30, 2030.

7 (5) This section expires June 30, 2031.

8 NEW SECTION. **Sec. 14.** If any provision of this act or its  
9 application to any person or circumstance is held invalid, the  
10 remainder of the act or the application of the provision to other  
11 persons or circumstances is not affected.

12 NEW SECTION. **Sec. 15.** Sections 1 through 12 of this act  
13 constitute a new chapter in Title 19 RCW.

--- END ---

8

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

**GOODRX HOLDINGS, INC.,** a corporation,  
also d/b/a GoodRx, GoodRx Gold, GoodRx  
Care, HeyDoctor, and HeyDoctor by  
GoodRx;

Defendant.

**Case No. 3:23-cv-460**

**STIPULATED ORDER FOR  
PERMANENT INJUNCTION,  
CIVIL PENALTY JUDGMENT,  
AND OTHER RELIEF**

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission (“Commission” or “FTC”), filed its Complaint for Permanent Injunction, Civil Penalties, and Other Relief (“Complaint”) in this matter, pursuant to Sections 5(a)(1), 5(m)(1)(A), 13(b), 16(a)(1), and 19 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), 56(a)(1), 57b, and the Health Breach Notification Rule (“HBNR”), 16 C.F.R. § 318. Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief (“Order”) to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

**FINDINGS**

1. This Court has jurisdiction over this matter.
2. The Complaint charges that Defendant participated in deceptive and unfair acts or

1 practices in violation of Section 5 of the FTC Act in the disclosure of health and personal  
2 information to third parties, the failure to limit third-party use of health information, the  
3 misrepresentation of compliance with the Digital Advertising Alliance principles, the  
4 misrepresentation that consumer’s health information was protected under the Health Insurance  
5 Portability and Accountability Act (“HIPAA”), the failure to implement sufficient policies or  
6 procedures to prevent the improper or unauthorized disclosure of health information, or to notify  
7 users of breaches of that information, and the failure to provide notice and obtain consent before  
8 the use and disclosure of health information for advertising. The Complaint also charges that  
9 Defendant violated the HBNR by failing to notify individuals and the Commission of a Breach  
10 of Security of Unsecured PHR Identifiable Health Information (as defined herein).

11 3. Defendant neither admits nor denies any of the allegations in the Complaint,  
12 except as specifically stated in this Order. Only for purposes of this action, Defendant admits the  
13 facts necessary to establish jurisdiction.

14 4. Defendant waives any claim that it may have under the Equal Access to Justice  
15 Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order,  
16 and agrees to bear its own costs and attorney fees. Defendant waives and releases any claims  
17 that it may have against Plaintiff that relate to this action. The parties agree that this Order  
18 resolves all allegations in the Complaint.

19 5. Defendant and the Plaintiff waive all rights to appeal or otherwise challenge or  
20 contest the validity of this Order.

21 **DEFINITIONS**

22 For the purpose of this Order, the following definitions apply:

23 A. “**Affirmative Express Consent**” means any freely given, specific, informed and  
24 unambiguous indication of an individual’s wishes demonstrating agreement by the individual,  
25 such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the  
26 individual, apart from any “privacy policy,” “terms of service,” “terms of use,” or other similar  
27 document, of all information material to the provision of consent. Acceptance of a general or  
28 broad terms of use or similar document that contains descriptions of agreement by the individual

1 along with other, unrelated information, does not constitute Affirmative Express Consent.  
2 Hovering over, muting, pausing, or closing a given piece of content does not constitute  
3 Affirmative Express Consent. Likewise, agreement obtained through use of user interface  
4 designed or manipulated with the substantial effect of subverting or impairing user autonomy,  
5 decision-making, or choice, does not constitute Affirmative Express Consent.

6 B. “**App Event**” means any data disclosed to, or collected by, a Third Party via its  
7 Software Development Kit, application programming interface, pixel, or other method for tracking  
8 users’ interactions with Defendant’s services or products.

9 C. “**Breach of Security**” means with respect to Unsecured PHR Identifiable Health  
10 Information of an individual in a Personal Health Record, acquisition of such information  
11 without the authorization of the individual. Unauthorized acquisition will be presumed to  
12 include unauthorized access to Unsecured PHR identifiable health information unless the vendor  
13 of personal health records, PHR related entity, or third party service provider that experienced  
14 the breach has reliable evidence showing that there has not been, or could not reasonably have  
15 been, unauthorized acquisition of such information.

16 D. “**Clear and Conspicuous**” or “**Clearly and Conspicuously**” means that a  
17 required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by  
18 ordinary consumers, including in all of the following ways:

19 1. In any communication that is solely visual or solely audible, the disclosure must  
20 be made through the same means through which the communication is presented. In any  
21 communication made through both visual and audible means, such as a television advertisement,  
22 the disclosure must be presented simultaneously in both the visual and audible portions of the  
23 communication even if the representation requiring the disclosure (“triggering representation”) is  
24 made through only one means.

25 2. A visual disclosure, by its size, contrast, location, the length of time it appears,  
26 and other characteristics, must stand out from any accompanying text or other visual elements so  
27 that it is easily noticed, read, and understood.

28 3. An audible disclosure, including by telephone or streaming video, must be

1 delivered in a volume, speed, and cadence sufficient for ordinary consumers to hear it easily and  
2 understand it.

3 4. In any communication using an interactive electronic medium, such as the  
4 Internet or software, the disclosure must be unavoidable.

5 5. The disclosure must use diction and syntax understandable to ordinary consumers  
6 and must appear in each language in which the triggering representation appears.

7 6. The disclosure must comply with these requirements in each medium through  
8 which it is received, including all electronic devices and face-to-face communications.

9 7. The disclosure must not be contradicted or mitigated by, or inconsistent with,  
10 anything else in the communication.

11 8. When the representation or sales practice targets a specific audience, such as  
12 children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of  
13 that group.

14 E. “**Defendant**” means GoodRx Holdings, Inc., doing business as GoodRx, GoodRx  
15 Gold, GoodRx Care, HeyDoctor, HeyDoctor by GoodRx, its successors and assigns, and its  
16 wholly or partially owned subsidiaries, including GoodRx Intermediate Holdings, Inc., GoodRx,  
17 Inc., Iodine, Inc., HeyDoctor, LLC, Lighthouse Acquisition Corp., Scriptcycle, LLC,  
18 HealthiNation, Inc., Buckeye Acquisition, LLC, RxSaver, Inc., flipMD, Inc., Pharmacy Services,  
19 LLC, and VitaCare Prescription Services, Inc.

20 F. “**Covered Business**” means Defendant and any business that Defendant controls,  
21 directly or indirectly.

22 G. “**Covered Incident**” means any instance of a violation of Section I, II, or III of  
23 this Order.

24 H. “**Covered Information**” means information from or about an individual  
25 consumer, including but not limited to Personal Information, Health Information, or PHR  
26 Identifiable Health Information.

27 I. “**Covered User**” means any individual who used Defendant’s websites or  
28 downloaded Defendant’s mobile applications between July 2017 through April 2020.

1 J. **“Delete” “Deleted” or “Deletion”** means to remove information such that it is not  
2 maintained in retrievable form and cannot be retrieved in the normal course of business.

3 K. **“Health Care Provider”** means a provider of services (as defined in 42 U.S.C. §  
4 1395x(u)), a provider of medical or other services (as defined in 42 U.S.C. § 1395x(s)), and any  
5 other person furnishing healthcare services or supplies.

6 L. **“Health Information”** means individually identifiable information relating to the  
7 past, present, or future physical or mental health or conditions of an individual, the provision of  
8 health care to an individual, or the past, present, or future payment for the provision of health  
9 care to an individual; and any individually identifiable health information that is derived or  
10 extrapolated from information about an individual’s activities, or pattern of activities, from  
11 which a determination is made that the individual has a health condition or is taking a drug.

12 M. **“Individually Identifiable Health Information”** means any information,  
13 including demographic information collected from an individual, that: (1) is created or received  
14 by a Health Care Provider, health plan, employer, or health care clearinghouse; and (2) relates to  
15 the past, present, or future physical or mental health or condition of an individual, the provision  
16 of health care to an individual, or the past, present, or future payment for the provision of health  
17 care to an individual, and: (a) identifies the individual; or (b) with respect to which there is a  
18 reasonable basis to believe that the information can be used to identify the individual.

19 N. **“Personal Health Record”** means an electronic record of PHR Identifiable  
20 Health Information on an individual that can be drawn from multiple sources and that is  
21 managed, shared, and controlled by or primarily for the individual.

22 O. **“Personal Information”** means any individually identifiable information about  
23 an individual collected online, including: (1) a first and last name; (2) home or other physical  
24 address including street name and name of a city or town; (3) online contact information,  
25 meaning an email address or any other substantially similar identifier that permits direct contact  
26 with a person online, including but not limited to an instant messaging user identifier, a voice  
27 over internet protocol (VOIP) identifier, or a video chat identifier; (4) a screen or user name  
28 where it functions in the same manner as online contact information; (5) a telephone number; (6)

1 a Social Security number; (7) a persistent identifier that can be used to recognize a user over time  
2 and across different websites or online services, including but not limited to a customer number  
3 held in a “cookie,” an Internet Protocol (“IP”) address, a mobile device ID, a processor or device  
4 serial number, or unique identifier; (8) geolocation information sufficient to identify street name  
5 and name of a city or town; (9) a driver’s license or other government-issued identification  
6 number; (10) a financial institution account number; (11) credit or debit card information; or  
7 (12) any information combined with any of (1) through (11) above.

8 P. **“PHR Identifiable Health Information”** means Individually Identifiable Health  
9 Information and, with respect to an individual, information: (1) that is provided by or on behalf  
10 of the individual; and (2) that identifies the individual or with respect to which there is a  
11 reasonable basis to believe that the information can be used to identify the individual.

12 Q. **“Third Party”** or **“Third Parties”** means any individual or entity other than: (1)  
13 Defendant; (2) an entity with which Defendant has a business associate agreement complying  
14 with 45 C.F.R. Part 164.504(e)(2)(ii)(A); (3) a pharmacy facilitating the consumer obtaining a  
15 discount for a prescription or medical services; (4) a service provider or partner of Defendant  
16 that: (i) uses or receives Covered Information collected by or on behalf of Defendant for and at  
17 the direction of Defendant and no other individual or entity, or to process, provide access to, or  
18 facilitate transactions for prescriptions, treatments, or medical services; (ii) does not disclose the  
19 data, or any individually identifiable information derived from such data, to any individual or  
20 entity other than Defendant or a subcontractor to such service provider or partner bound to data  
21 processing terms no less restrictive than terms to which the service provider or partner is bound,  
22 unless for the specific purpose of performing the services specified in the contract; and (iii) does  
23 not use the data for any purpose other than the purposes in (Q)(4)(i) or for internal use to  
24 provide, maintain, improve, or secure the services provided to Defendant, provided that internal  
25 use does not include using Covered Information obtained from Defendant to build or modify  
26 household or consumer profiles to use in providing services to another business, or to correct or  
27 augment data acquired from another source; or (5) any entity that uses Covered Information only  
28 as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to



1 enforce Defendant’s terms of use, or (iii) to detect, prevent, or mitigate fraud or security  
2 vulnerabilities.

3 R. “**Unsecured**” means PHR Identifiable Health Information that is not protected  
4 through the use of a technology or methodology specified by the Secretary of Health and Human  
5 Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and  
6 Recovery Act of 2009.

7 **ORDER**

8 **I. BAN ON DISCLOSURE OF HEALTH INFORMATION FOR ADVERTISING**  
9 **PURPOSES**

10 IT IS ORDERED that:

11 A. Defendant, Defendant’s officers, agents, employees, and attorneys who receive  
12 actual notice of this Order, whether acting directly or indirectly, are permanently restrained and  
13 enjoined from disclosing Health Information to Third Parties for Advertising Purposes.

14 B. For purposes of this Section, “Advertising Purposes” means advertising,  
15 marketing, promoting, offering, offering for sale, or selling any products or services on, or  
16 through Third Party websites, mobile applications, or services. Advertising Purpose shall not  
17 include: (i) reporting and analytics related to understanding advertising and advertising  
18 effectiveness, such as statistical reporting, traffic analysis, understanding the number of and type  
19 of ads served, or conversion measurement; or (ii) communications, services, or products  
20 requested by a consumer that are sent or provided to the consumer; or (iii) contextual advertising,  
21 meaning non-personalized advertising shown as part of a consumer’s current interaction with  
22 Defendant’s websites or mobile applications, provided that the consumer’s Covered Information  
23 is not disclosed to another Third Party and is not used to build a profile about the consumer or  
24 otherwise alter the consumer’s experience outside the current interaction with Defendant’s  
25 websites or mobile application.

26 C. For purposes of this Section, Health Information shall not include (a) a pharmacy  
27 name (except for any specialty or other pharmacies that provide medications or services that are  
28 limited to treating a specific health condition); or (b) general engagement with or use of

1 Defendant's services or content, such as accessing general pricing information, provided that  
2 such engagement or use does not reveal an individual's Personal Information combined with (i)  
3 information about a medication or class of medication(s) that an individual is prescribed, has  
4 purchased, or is taking steps to purchase or obtain by accessing, downloading, or requesting a  
5 coupon, or taking other steps to purchase or obtain such medication or class of medication(s), or  
6 (ii) information that reveals an individual's health status, or that an individual has or is seeking  
7 treatment for a specific health condition or conditions.

8 **II. PROHIBITION AGAINST MISREPRESENTATIONS**

9 IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees,  
10 and attorneys, and all other persons in active concert or participation with any of them, who  
11 receive actual notice of this Order, whether acting directly or indirectly, in connection with  
12 promoting or offering for sale any product or service are permanently restrained and enjoined  
13 from misrepresenting or assisting others in misrepresenting, expressly or by implication:

14 A. the purposes for which Defendant or any entity to whom it discloses Covered  
15 Information collects, maintains, uses, or discloses Covered Information;

16 B. the extent to which consumers may exercise control over Defendant's collection,  
17 maintenance, use, disclosure, or Deletion of Covered Information, and the steps a consumer must  
18 take to implement such controls;

19 C. the extent to which Defendant is a member of, adheres to, complies with, is  
20 certified by, is endorsed by, or otherwise participates in any privacy, security, or any other  
21 compliance program sponsored by a government or any self-regulatory or standard-setting  
22 organization, including the Digital Advertising Alliance, the Digital Advertising Accountability  
23 Program, or any entity that certifies compliance with HIPAA;

24 D. the extent to which Defendant is a HIPAA-covered entity, and the extent that  
25 Defendant's privacy and information practices are in compliance with HIPAA requirements; and

26 E. the extent to which Defendant collects, maintains, uses, discloses, Deletes, or  
27 permits or denies access to any Covered Information, or the extent to which Defendant protects  
28 the availability, confidentiality, or integrity of any Covered Information.

1           **III.    PROHIBITION AGAINST DISCLOSURE OF HEALTH INFORMATION**  
2                           **WITHOUT AFFIRMATIVE EXPRESS CONSENT AND NOTICE**

3           IT IS FURTHER ORDERED that:

4           A.       Defendant, Defendant’s officers, agents, employees, and attorneys, and all other  
5 persons in active concert or participation with any of them who receive actual notice of this  
6 Order, whether acting directly or indirectly, in connection with the sale of any product or service,  
7 are permanently restrained and enjoined from disclosing Health Information to Third Parties for  
8 Non-Advertising Purposes without first obtaining Affirmative Express Consent.

9           B.       For purposes of this Section, Non-Advertising Purposes means all purposes other  
10 than: (i) Advertising Purposes as defined in Section I of this Order; (ii) communications,  
11 services, or products requested by a consumer that are sent or provided by Defendant directly to  
12 the consumer, such as Defendant texting, emailing, or mailing a consumer, or showing content  
13 on Defendant’s own properties to a consumer; and (iii) contextual advertising, meaning non-  
14 personalized advertising shown as part of a consumer’s current interaction with Defendant’s  
15 websites or mobile applications, including associated ad serving and response mechanisms,  
16 provided that the consumer’s Covered Information is not disclosed to another Third Party and is  
17 not used to build a profile about the consumer or otherwise alter the consumer’s experience  
18 outside the current interaction with Defendant’s websites or mobile applications.

19           C.       For purposes of this Section, Health Information shall not include (a) a pharmacy  
20 name (except for any specialty or other pharmacies that provide medications or services that are  
21 limited to treating a specific health condition); or (b) general engagement with or use of  
22 Defendant’s services or content, such as accessing general pricing information, provided that  
23 such engagement or use does not reveal an individual’s Personal Information combined with (i)  
24 information about a medication or class of medication(s) that an individual is prescribed, has  
25 purchased, or is taking steps to purchase or obtain by accessing, downloading, or requesting a  
26 coupon, or taking other steps to purchase or obtain such medication or class of medication(s), or  
27 (ii) information that reveals an individual’s health status, or that an individual has or is seeking  
28 treatment for a specific health condition or conditions.

1 D. When obtaining Affirmative Express Consent required under this Section,  
2 Defendant must provide notice Clearly and Conspicuously that states the categories of Health  
3 Information that will be disclosed to Third Parties, the identities of such Third Parties (where a  
4 consumer is using a physical, non-electronic discount card, Defendant need only disclose the  
5 category of such Third Parties), and all purposes for Defendant’s disclosure of such Health  
6 Information, including how it may be used by each Third Party.

7 E. It shall not be a violation of this Section if Defendant discloses Health  
8 Information to Third Parties for Non-Advertising Purposes without first obtaining Affirmative  
9 Express Consent, if Defendant proves that: (1) the information is “protected health information,”  
10 defined under 45 C.F.R. Section 160.103, and pursuant to the Health Insurance Portability and  
11 Accountability Act of 1996, as amended, including by the Health Information Technology for  
12 Economic and Clinical Health Act (“HITECH”) (collectively, “HIPAA”); (2) Defendant made  
13 such disclosure in its capacity as a covered entity or business associate, as defined under 45  
14 C.F.R. Section 160.103; and (3) any such disclosure was either required or permitted under 45  
15 C.F.R. Part 160 and Part 164, Subparts A and E (the “HIPAA Privacy Rule”).

16 **IV. HEALTH BREACH NOTIFICATIONS**

17 IT IS FURTHER ORDERED that:

18 A. Defendant, for any Covered Business, following the discovery of a Breach of  
19 Security of Unsecured PHR Identifiable Health Information that is in a Personal Health Record  
20 maintained or offered by Defendant (including, but not limited to, the GoodRx, GoodRx Gold,  
21 GoodRx Care, and/or HeyDoctor websites or mobile applications), shall:

22 1. notify each individual who is a citizen or resident of the United States whose  
23 Unsecured PHR Identifiable Health Information was acquired by an unauthorized person as a  
24 result of such Breach of Security;

25 2. notify the Federal Trade Commission, in accordance with Subsection IV(E)  
26 below; or

27 3. notify prominent media outlets in a state or jurisdiction, if the Unsecured PHR  
28 Identifiable Health Information of five hundred (500) or more residents of such state or

1 jurisdiction is, or is reasonably believed to have been, acquired during such Breach of Security.

2 B. For the purposes of this Section, a Breach of Security shall be treated as  
3 discovered as of the first day on which such breach is known or reasonably should have been  
4 known to Defendant. Defendant shall be deemed to have knowledge of a Breach of Security if  
5 such breach is known, or reasonably should have been known, to any person, other than the  
6 person committing the breach, who is an employee, officer, or other agent of Defendant.

7 C. Except as otherwise provided, all notifications to individuals or the media  
8 required under this Section shall be sent without unreasonable delay and in no case later than  
9 sixty (60) calendar days after the discovery of the Breach of Security. If a law enforcement  
10 official determines that a notification, notice, or posting required under this Section would  
11 impede a criminal investigation or cause damage to national security, such notification, notice, or  
12 posting shall be delayed. This Subsection shall be implemented in the same manner as provided  
13 under 45 C.F.R. Section 164.528(a)(2), in the case of a disclosure covered under such section.

14 D. If Defendant provides notice under Subsection IV(A)(1), it shall do so by  
15 providing it in the following form:

16 1. Written notice, by first-class mail to the individual at the last known address of  
17 the individual, or by email or within-application messaging, if the individual is given a clear,  
18 conspicuous, and reasonable opportunity to receive notification by first-class mail, and the  
19 individual does not exercise that choice. If the individual is deceased, Defendant must provide  
20 such notice to the next of kin of the individual if the individual had provided contact information  
21 for his or her next of kin, along with authorization to contact them. The notice may be provided  
22 in one or more mailings as information is available.

23 2. If, after making reasonable efforts to contact all individuals to whom notice is  
24 required under Subsection IV(A)(1), through the means provided in Subsection IV(D)(1),  
25 Defendant finds that contact information for ten (10) or more individuals is insufficient or out-of-  
26 date, Defendant shall provide substitute notice, which shall be reasonably calculated to reach the  
27 individuals affected by the Breach of Security, in the following form:

28 a. Through a conspicuous posting for a period of ninety (90) days on the

1 home page of its website; or

2 b. In major print or broadcast media, including major media in geographic  
3 areas where the individuals affected by the Breach of Security likely  
4 reside. Such a notice in media or web posting shall include a toll-free  
5 phone number, which shall remain active for at least ninety (90) days,  
6 where an individual can learn whether or not the individual's PHR  
7 Identifiable Health Information may be included in the Breach of Security.

8 3. In any case deemed by Defendant to require urgency because of possible  
9 imminent misuse of Unsecured PHR Identifiable Health Information, Defendant may provide  
10 information to individuals by telephone or other means, as appropriate, in addition to notice  
11 provided under Subsection IV(E)(1).

12 E. Defendant shall, in accordance with Subsection IV(A)(2), provide notice to the  
13 Federal Trade Commission following the discovery of a Breach of Security. If the Breach of  
14 Security involves the Unsecured PHR Identifiable Health Information of five hundred (500) or  
15 more individuals, then such notice shall be provided as soon as possible and in no case later than  
16 ten (10) business days following the date of discovery of the Breach of Security. If the Breach of  
17 Security involves the Unsecured PHR Identifiable Health Information of fewer than five hundred  
18 (500) individuals, Defendant may maintain a log of any such Breach of Security, and submit  
19 such a log annually to the Federal Trade Commission no later than sixty (60) calendar days  
20 following the end of the calendar year, documenting Breaches of Security from the preceding  
21 calendar year. Unless otherwise directed by a Commission representative in writing, Defendant  
22 must submit all notices and logs required under this Section to: DEbrief@ftc.gov or sent by  
23 overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of  
24 Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington,  
25 DC 20580. The subject line must begin: "U.S. v. GoodRx Holdings, Inc."

26 F. Regardless of the method by which notice is provided to individuals, the Federal  
27 Trade Commission, or the media under this Section, notice of a Breach of Security shall be in  
28 plain language and include, to the extent possible, the following:



1 Complaint Entities, provide a copy of the Complaint and Order to all Third Parties and  
2 Complaint Entities that received Health Information of Covered Users, notify all such Third  
3 Parties and Complaint Entities in writing that the Federal Trade Commission alleges that  
4 Defendant disclosed Covered Information of Covered Users to them in a manner that was unfair  
5 or deceptive and in violation of the FTC Act, instruct all such Third Parties and Complaint  
6 Entities to Delete all Covered Information of Covered Users received from Defendant, and  
7 demand written confirmation that all the identified Covered Information has been Deleted.  
8 Defendant's instruction to each such Third Party and Complaint Entities shall include a  
9 description of the Covered Information of Covered Users shared with the Third Party or  
10 Complaint Entities. Defendant must provide all instructions sent to the Third Parties and  
11 Complaint Entities to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal  
12 Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade  
13 Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must  
14 begin: "U.S. v. GoodRx Holdings, Inc."

15 B. Defendant shall not disclose any Covered Information in any form, including  
16 hashed or encrypted Covered Information, to any Third Party or Complaint Entities identified in  
17 Subsection A above until Defendant confirms each Third Party and Complaint Entity's receipt of  
18 the instructions required by Subsection A above. Defendant must provide all receipts of  
19 confirmation and any responses from Third Parties or Complaint Entities within five (5) days of  
20 receipt to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to:  
21 Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade  
22 Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must  
23 begin: "U.S. v. GoodRx Holdings, Inc."

24 C. Defendant shall not use any Third Party or Complaint Entity identified in  
25 Subsection A above to advertise, market, promote, offer, offer for sale, or sell any product or  
26 service until Defendant confirms each Third Party and Complaint Entity's receipt of the  
27 instructions required by Subsection A above.  
28



**VII. MANDATED PRIVACY PROGRAM**

IT IS FURTHER ORDERED that any Covered Business, in connection with the collection, maintenance, use, disclosure of, or provision of access to, Covered Information, must, within one hundred eighty (180) days of entry of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program (“Privacy Program”) that protects the privacy, security, availability, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Privacy Program;

B. Provide the written program and any evaluations thereof or updates thereto to each Covered Business’s board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the Covered Business’s Privacy Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

C. Designate a qualified employee or employees, who report(s) directly to the Chief Executive Officer(s) or, in the event a Chief Executive Officer role does not exist, a similarly-situated executive, to coordinate and be responsible for the Privacy Program; and keep the Chief Executive Officer(s) and Board of Directors informed of the Privacy Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks in each area of the Covered Business’s operations to the privacy, security, availability, confidentiality, and integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of, or provision of access to, Covered Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information identified by each Covered Business in response to Subsection VII.D.

1 Each safeguard must be based on the volume and sensitivity of the Covered Information that is at  
2 risk, and the likelihood that the risk could be realized and result in the unauthorized access,  
3 collection, use, destruction, disclosure of, or provision of access to, the Covered Information.

4 Such safeguards must also include:

5 1. policies, procedures, and technical measures to systematically inventory Covered  
6 Information in the Covered Business's control and Delete Covered Information that is no longer  
7 necessary;

8 2. policies, procedures, and technical measures to prevent the collection,  
9 maintenance, use, or disclosure of, or provision of access to, Covered Information inconsistent  
10 with the Covered Business's representations to consumers;

11 3. audits, assessments, and reviews of the contracts, privacy policies, and terms of  
12 service associated with any Third Party to which each Covered Business discloses, or provides  
13 access to Covered Information;

14 4. policies, procedures, and controls to ensure that each Covered Business complies  
15 with Sections I-IV above;

16 5. policies and technical measures that limit employee and contractor access to  
17 Covered Information to only those employees and contractors with a legitimate business need to  
18 access such Covered Information;

19 6. mandatory privacy training programs for all employees on at least an annual  
20 basis, updated to address: the collection, use, and disclosure of Covered Information; any internal  
21 or external risks identified by each Covered Business in Subsection VII(D); and safeguards  
22 implemented pursuant to Subsection VII(E), that includes training on the requirements of this  
23 Order;

24 7. a data retention policy that, at a minimum, includes:

- 25 a. a retention schedule that limits the retention of Covered Information for  
26 only as long as is reasonably necessary to fulfill the purpose for which the  
27 Covered Information was collected; provided, however, that such Covered  
28 Information need not be destroyed, and may be disclosed, to the extent

1 requested by a government agency or required by law, regulation, or court  
2 order; and

3 b. a requirement that each Covered Business document, adhere to, and make  
4 publicly available in its terms of service or terms of use a retention  
5 schedule for Covered Information, setting forth: (1) the purposes for  
6 which such information is collected; (2) the specific business need for  
7 retaining each type of Covered Information; and (3) a set timeframe for  
8 Deletion of each type of Covered Information (absent any intervening  
9 Deletion requests from consumers) that precludes indefinite retention of  
10 any Covered Information;

11 8. For each product or service, policies and procedures to document internally the  
12 decision to collect, use, disclose, or maintain each type of Covered Information. Such  
13 documentation should include: (a) the name or names of the person or people who made the  
14 decision; (b) for what purpose the type of Covered Information is being collected; (c) the data  
15 segmentation controls in place to ensure that the type of Covered Information collected is only  
16 used for the particular purpose for which it was collected; (d) the data retention limit set for each  
17 type of Covered Information and the technical means for achieving Deletion; (e) the safeguards  
18 in place to prevent disclosure or sale of each type of Covered Information; and (f) the access  
19 controls in place to ensure only authorized employees with a need-to-know have access to each  
20 type of Covered Information;

21 9. audits, assessments, reviews, or testing of web pixels and Software Development  
22 Kits, and their associated Third Parties, to which each Covered Business discloses or provides  
23 access to Covered Information.

24 F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty  
25 (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the  
26 internal and external risks to the privacy, security, availability, confidentiality, and integrity of  
27 Covered Information, and modify the Privacy Program based on the results;

1 G. Test and monitor the effectiveness of the safeguards at least once every twelve  
2 (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and  
3 modify the Privacy Program based on the results;

4 H. Select and retain service providers capable of safeguarding Covered Information  
5 they receive from the Covered Business, and contractually require service providers to  
6 implement and maintain safeguards for Covered Information;

7 I. Evaluate and adjust the Privacy Program in light of any material changes to each  
8 Covered Business's operations or business arrangements, the results of the testing and  
9 monitoring required by Subsection VII(F), a Covered Incident, new or more efficient  
10 technological or operational methods to control for the risks identified in Subsection VII(D), and  
11 any other circumstances that the Covered Business knows or has reason to believe may have a  
12 material impact on the effectiveness of the Privacy Program or any of its individual safeguards.  
13 The Covered Business may make this evaluation and adjustment to the Privacy Program at any  
14 time, but must, at a minimum, evaluate the Privacy Program at least once every twelve (12)  
15 months and modify the Program as necessary based on the results.

16 **VIII. PRIVACY ASSESSMENT BY A THIRD PARTY**

17 IT IS FURTHER ORDERED that, in connection with compliance with Section VII, for  
18 any Covered Business that collects, maintains, uses, discloses, or provides access to Covered  
19 Information, Defendant must obtain initial and biennial assessments ("Assessments"):

20 A. The Assessments must be obtained from one or more qualified, objective,  
21 independent third-party professionals ("Assessor(s)") who: (1) uses procedures and standards  
22 generally accepted in the profession; (2) conducts an independent review of the Privacy  
23 Program; (3) retains all documents relevant to each Assessment for five (5) years after  
24 completion of such Assessment; and (4) will provide such documents to the Commission within  
25 ten (10) days of receipt of a written request from a representative of the Commission. No  
26 documents may be withheld on the basis of a claim of confidentiality, proprietary or trade  
27 secrets, work product protection, attorney client privilege, statutory exemption, or any similar  
28 claim. The Assessor(s) must have a minimum of three (3) years of experience in the field of

1 privacy and data protection.

2 B. For each Assessment, Defendant must provide the Associate Director for  
3 Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the  
4 name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall  
5 have the authority to approve in his or her sole discretion.

6 C. The reporting period for the Assessments must cover: (1) the first year after the  
7 entry of this Order for the initial Assessment; and (2) each two (2) year period thereafter for  
8 twenty (20) years after the entry of this Order for the biennial Assessments.

9 D. Each Assessment must, for the entire assessment period:

10 E. determine whether Defendant has implemented and maintained the Privacy  
11 Program required by Section VII;

12 F. assess the effectiveness of Defendant's implementation and maintenance of  
13 Subsections VII(A)-(I);

14 G. identify any gaps or weaknesses in the Privacy Program or instances of material  
15 noncompliance with Subsections VII(A)-(I);

16 H. address the status of gaps or weaknesses in the Privacy Program, as well as any  
17 instances of material non-compliance with Subsections VII(A)-(I), that were identified in any  
18 prior Assessment required by this Order; and

19 I. identify specific evidence (including, but not limited to, documents reviewed,  
20 sampling and testing performed, and interviews conducted) examined to make such  
21 determinations, assessments, and identifications, and explain why the evidence that the Assessor  
22 examined is: (a) appropriate for assessing an enterprise of Defendant's size, complexity, and risk  
23 profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall  
24 rely solely on assertions or attestations by Defendant, Defendant's management, or a Covered  
25 Business's management. The Assessment must be signed by the Assessor, state that the  
26 Assessor conducted an independent review of the Privacy Program and did not rely solely on  
27 assertions or attestations by Defendant, Defendant's management, or a Covered Business's  
28 management and state the number of hours that each member of the Assessor's assessment team

1 worked on the Assessment. To the extent Defendant revises, updates, or adds one or more  
 2 safeguards required under Subsection VII(E) in the middle of an Assessment period, the  
 3 Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the  
 4 time period in which it was in effect, and provide a separate statement detailing the basis for each  
 5 revised, updated, or additional safeguard.

6 J. Each Assessment must be completed within sixty (60) days after the end of the  
 7 reporting period to which the Assessment applies. Unless otherwise directed by a Commission  
 8 representative in writing, Defendant must submit the initial Assessment to the Commission  
 9 within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or  
 10 by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,  
 11 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,  
 12 Washington, DC 20580. The subject line must begin, "U.S. v. GoodRx Holdings, Inc." All  
 13 subsequent biennial Assessments must be retained by Defendant until the Order is terminated  
 14 and provided to the Associate Director for Enforcement within ten (10) days of request.

#### 15 IX. COOPERATION WITH ASSESSOR

16 IT IS FURTHER ORDERED that Defendant, whether acting directly or indirectly, in  
 17 connection with the Assessments required by Section VIII, must:

18 A. provide or otherwise make available to the Assessor all information and material  
 19 in their possession, custody, or control that is relevant to the Assessment for which there is no  
 20 reasonable claim of privilege;

21 B. provide or otherwise make available to the Assessor information about all  
 22 Covered Information in Defendant's custody or control so that the Assessor can determine the  
 23 scope of the Assessment; and

24 C. disclose all material facts to the Assessor, and not misrepresent in any manner,  
 25 expressly or by implication, any fact material to the Assessor's: (1) determination of whether  
 26 Defendant has implemented and maintained the Privacy Program required by Section VII; (2)  
 27 assessment of the effectiveness of the implementation and maintenance of Subsections VII(A)-  
 28 (I); or (3) identification of any gaps or weaknesses in, or instances of material noncompliance

1 with, the Privacy Program required by Section VII.

2 **X. ANNUAL CERTIFICATION**

3 IT IS FURTHER ORDERED that Defendant must:

4 A. One year after the entry of this Order, and each year thereafter, provide the  
5 Commission with a certification from a senior corporate manager, or, if no such senior corporate  
6 manager exists, a senior officer of each Covered Business that: (1) the Covered Business has  
7 established, implemented, and maintained the requirements of this Order; (2) the Covered  
8 Business is not aware of any material noncompliance that has not been: (a) corrected, or (b)  
9 disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The  
10 certification must be based on the personal knowledge of the senior corporate manager, senior  
11 officer, or subject matter experts upon whom the senior corporate manager or senior officer  
12 reasonably relies in making the certification.

13 B. Unless otherwise directed by a Commission representative in writing, submit all  
14 annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or  
15 by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau  
16 of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,  
17 Washington, D.C. 20580. The subject line must begin, "U.S. v. GoodRx Holdings, Inc."

18 **XI. COVERED INCIDENT REPORTS**

19 IT IS FURTHER ORDERED that Defendant, within thirty (30) days after discovery of a  
20 Covered Incident, must submit a report to the Commission, unless the Covered Incident also  
21 constitutes a Breach of Security involving the Unsecured PHR Identifiable Health Information of  
22 500 or more individuals and therefore requiring notice under Section IV of this Order. The  
23 report must include, to the extent possible:

24 A. the date, estimated date, or estimated date range when the Covered Incident  
25 occurred;

26 B. a description of the facts relating to the Covered Incident, including the causes  
27 and scope of the Covered Incident, if known;

28 C. the number of consumers whose information was affected;

1 D. the acts that Defendant has taken to date to remediate the Covered Incident;  
2 protect Covered Information from further disclosure, exposure, or access; and protect affected  
3 individuals from identity theft or other harm that may result from the Covered Incident; and

4 E. a representative copy of any materially different notice sent by Defendant to  
5 consumers or to any U.S. federal, state, or local government entity.

6 Unless otherwise directed by a Commission representative in writing, all Covered  
7 Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov  
8 or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,  
9 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,  
10 Washington, DC 20580. The subject line must begin: "U.S. v. GoodRx Holdings, Inc."

11 **XII. MONETARY JUDGMENT FOR CIVIL PENALTY**

12 IT IS FURTHER ORDERED that:

13 A. Judgment in the amount of \$1,500,000 is entered in favor of Plaintiff against  
14 Defendant as a civil penalty.

15 B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of  
16 the United States, \$1,500,000, which, as Defendant stipulates, their undersigned counsel holds in  
17 escrow for no purpose other than payment to Plaintiff. Such payment must be made within 7  
18 days of entry of this Order by electronic fund transfer in accordance with instructions previously  
19 provided by a representative of Plaintiff.

20 **XIII. ADDITIONAL MONETARY PROVISIONS**

21 IT IS FURTHER ORDERED that:

22 A. Defendant relinquishes dominion and all legal and equitable right, title, and  
23 interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

24 B. The facts alleged in the Complaint will be taken as true, without further proof, in  
25 any subsequent civil litigation by or on behalf of the Commission, including in a proceeding to  
26 enforce its rights to any payment or monetary judgment pursuant to this Order.

27 C. Defendant acknowledges that its Taxpayer Identification Numbers, or Employer  
28 Identification Numbers, which Defendant previously submitted to the Commission, may be used



1 for collecting and reporting on any delinquent amount arising out of this Order, in accordance  
2 with 31 U.S.C. § 7701.

3 **XIV. ORDER ACKNOWLEDGMENTS**

4 IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this  
5 Order:

6 A. Defendant, within seven (7) days of entry of this Order, must submit to the  
7 Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

8 B. For 20 years after entry of this Order, for any business that Defendant is the  
9 majority owner or controls directly or indirectly, Defendant must deliver a copy of this Order to:  
10 (1) all principals, officers, directors, and LLC managers and members; (2) all employees having  
11 managerial responsibilities for conduct related to the subject matter of the Order and all agents  
12 and representatives who participate in conduct related to the subject matter of the Order; and (3)  
13 any business entity resulting from any change in structure as set forth in the Section titled  
14 Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for  
15 current personnel. For all others, delivery must occur before they assume their responsibilities.

16 C. From each individual or entity to which Defendant delivered a copy of this Order,  
17 Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of  
18 this Order.

19 **XV. COMPLIANCE REPORTING**

20 IT IS FURTHER ORDERED that Defendant make timely submissions to the  
21 Commission:

22 A. One year after entry of this Order, Defendant must submit a compliance report,  
23 sworn under penalty of perjury:

24 Defendant must: (a) identify the primary physical, postal, and email address and  
25 telephone number, as designated points of contact, which representatives of the  
26 Commission and Plaintiff may use to communicate with Defendant; (b) identify all of  
27 that Defendant's businesses by all of their names, telephone numbers, and physical,  
28 postal, email, and Internet addresses; (c) describe the activities of each business,

1 including the goods and services offered, and the means of advertising, marketing, and  
2 sales; (d) describe in detail whether and how Defendant is in compliance with each  
3 Section of this Order; and (e) provide a copy of each Order Acknowledgment obtained  
4 pursuant to this Order, unless previously submitted to the Commission.

5 B. One year after entry of this Order and annually thereafter for 5 years, Defendant  
6 must submit a supplemental compliance report, sworn under penalty of perjury, explaining any  
7 disclosure of Health Information to Third Parties for Non-Advertising Purposes that was made  
8 without first obtaining Affirmative Express Consent in violation of Section III of this Order and  
9 not in reliance on Subsection III.E of this Order, including: the type of information disclosed; the  
10 purpose for each such disclosure; the part of the Covered Business that made the disclosure, the  
11 reason the disclosure was in compliance with the HIPAA Privacy Rule; and the dates of the  
12 disclosure.

13 C. For 20 years after entry of this Order, Defendant must submit a compliance  
14 notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:

15 (a) any designated point of contact; or (b) the structure of Defendant or any entity that  
16 Defendant has any ownership interest in or controls directly or indirectly that may affect  
17 compliance obligations arising under this Order, including: creation, merger, sale, or  
18 dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or  
19 practices subject to this Order.

20 D. Defendant must submit to the Commission notice of the filing of any bankruptcy  
21 petition, insolvency proceeding, or similar proceeding by or against Defendant within fourteen  
22 (14) days of its filing.

23 E. Any submission to the Commission required by this Order to be sworn under  
24 penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by  
25 concluding: “I declare under penalty of perjury under the laws of the United States of America  
26 that the foregoing is true and correct. Executed on: \_\_\_\_\_” and supplying the date, signatory’s  
27 full name, title (if applicable), and signature.

28 F. Unless otherwise directed by a Commission representative in writing, all

1 submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or  
2 sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,  
3 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,  
4 Washington, DC 20580. The subject line must begin: “U.S. v. GoodRx Holdings, Inc.”

5 **XVI. RECORDKEEPING**

6 IT IS FURTHER ORDERED that Defendant must create certain records for twenty (20)  
7 years after entry of the Order, and retain each such record for five (5) years. Specifically,  
8 Defendant must create and retain the following records:

- 9 A. accounting records showing the revenues from all goods or services sold;
- 10 B. personnel records showing, for each person providing services, whether as an  
11 employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position;  
12 dates of service; and (if applicable) the reason for termination;
- 13 C. records of all consumer complaints and refund requests, whether received directly  
14 or indirectly, such as through a third party, and any response;
- 15 D. records describing all disclosures of Health Information or PHR Identifiable  
16 Health Information to Third Parties;
- 17 E. records describing all disclosures of App Events to Third Parties;
- 18 F. all records necessary to demonstrate full compliance with each provision of this  
19 Order, including all submissions to the Commission; and
- 20 G. a copy of each unique advertisement or other marketing material pertaining to a  
21 specific drug or medical condition, and any advertisement that makes claims about the privacy or  
22 security of consumers’ Health Information.
- 23 H. every six months, a screen capture of Defendant’s website and mobile application  
24 flows relating to users inputting Covered Information.

25 **XVII. COMPLIANCE MONITORING**

26 IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant’s compliance  
27 with this Order:

- 28 A. Within fourteen (14) days of receipt of a written request from a representative of

1 the Commission or Plaintiff, Defendant must: submit additional compliance reports or other  
2 requested information, which must be sworn under penalty of perjury; appear for depositions;  
3 and produce documents for inspection and copying. The Commission and Plaintiff are also  
4 authorized to obtain discovery, without further leave of court, using any of the procedures  
5 prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33,  
6 34, 36, 45, and 69.

7 B. For matters concerning this Order, the Commission and Plaintiff are authorized to  
8 communicate directly with Defendant. Defendant must permit representatives of the  
9 Commission and Plaintiff to interview any employee or other person affiliated with any  
10 Defendant who has agreed to such an interview. The person interviewed may have counsel  
11 present.

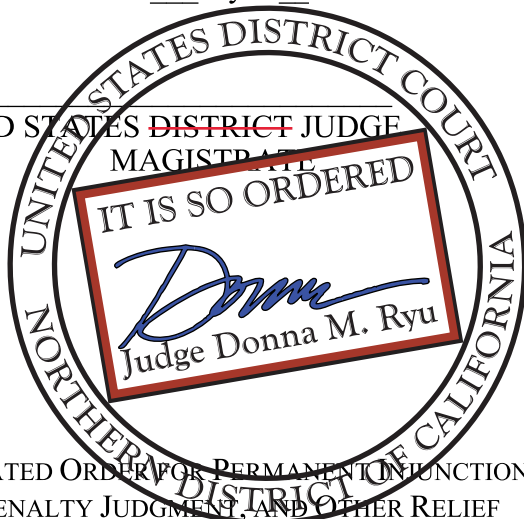
12 C. The Commission and Plaintiff may use all other lawful means, including posing,  
13 through its representatives as consumers, suppliers, or other individuals or entities, to Defendant  
14 or any individual or entity affiliated with Defendant, without the necessity of identification or  
15 prior notice. Nothing in this Order limits the Commission’s lawful use of compulsory process,  
16 pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

17 **XVIII. RETENTION OF JURISDICTION**

18 IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for  
19 purposes of construction, modification, and enforcement of this Order.

20 17th  
21 SO ORDERED this \_\_\_ day of February, 2023

22  
23 UNITED STATES DISTRICT JUDGE  
24 MAGISTRATE



25  
26  
27  
28 STIPULATED ORDER FOR PERMANENT INJUNCTION,  
CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

Case No. 3:23-cv-460

**SO STIPULATED AND AGREED:  
FOR PLAINTIFF UNITED STATES OF AMERICA:**

BRIAN M. BOYNTON  
Principal Deputy Assistant Attorney General  
Civil Division

ARUN G. RAO  
Deputy Assistant Attorney General, Consumer Protection Branch

AMANDA N. LISKAMM  
Acting Director, Consumer Protection Branch

LISA K. HSIAO  
Assistant Director, Consumer Protection Branch

/s/ Sarah Williams

Date: January 24, 2023

SARAH WILLIAMS  
Trial Attorney  
Consumer Protection Branch  
450 5<sup>th</sup> St NW, Suite 6400-S  
Washington, D.C. 20530  
Telephone: (202) 616-4269  
sarah.williams@usdoj.gov

STEPHANIE M. HINDS  
United States Attorney

/s/ Sharanya Mohan

SHARANYA MOHAN  
Assistant United States Attorney  
Northern District of California  
450 Golden Gate Avenue  
San Francisco, CA 94102  
Telephone: (415) 436-7198  
sharanya.mohan@usdoj.gov

**OF COUNSEL:**

RONNIE SOLOMON  
DENISE M. OKI  
Attorneys  
Federal Trade Commission  
Western Region San Francisco

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**FOR DEFENDANT:**

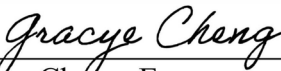


Date: 10/21/22

**Richard H. Cunningham**  
**Olivia Adendorff**  
**Rachael A. Rezabek**

Kirkland & Ellis, LLP  
Counsel for GoodRx Holdings, Inc.  
1301 Pennsylvania Ave., N.W. Washington, D.C. 20004  
(202) 425-5385  
[rich.cunningham@kirkland.com](mailto:rich.cunningham@kirkland.com)  
[olivia.adendorff@kirkland.com](mailto:olivia.adendorff@kirkland.com)  
[rachael.rezabek@kirkland.com](mailto:rachael.rezabek@kirkland.com)

**DEFENDANT: GoodRx Holdings, Inc.**



Date: October 21 2022

Gracye Cheng, Esq.  
Senior Vice President and General Counsel

## Exhibit A

### Website and Mobile Application Notice

The Federal Trade Commission alleges that we shared identifiable information about people who visited our website or used our app between July 2017 and April 2020 without their permission. This information included details about drug and health conditions people searched and their prescription medications. We shared this information with third parties, including Facebook. In some cases, GoodRx used the information to target people with health-related ads.

The Federal Trade Commission alleges we broke the law by sharing this health information without users' permission. To resolve the case, we have agreed to an FTC order [[notice will include a link to the FTC.gov page with Complaint and Order](#)] requiring that:

- We'll tell applicable third parties (like Facebook) who received that information to delete it.
- We'll never share your health information with applicable third parties (like Facebook) for advertising purposes.
- We won't share your health information with applicable third parties (like Facebook) for other purposes, unless we get your permission first.
- We'll put in place a comprehensive privacy program with heightened procedures and controls to protect your personal and health information. An independent auditor will review our program to make sure we're protecting your information. These audits will happen every two years for 20 years.

If you have any questions, email us at [privacy@goodrx.com](mailto:privacy@goodrx.com).

To learn more about the settlement, go to [ftc.gov](https://ftc.gov) and search for "GoodRx".

For advice on protecting your health privacy, read the FTC's [Does your health app protect your sensitive info?](#)

### Notice to Covered Users

The Federal Trade Commission alleges that between July 2017 and April 2020, you visited GoodRx.com or used the GoodRx app. During this time, we shared identifiable information related to you, including health information, without your permission. This information included details about drug and health conditions you searched and your prescription medications. We shared this information with third parties, including Facebook. In some cases, GoodRx used the information to target you with health-related ads.

The Federal Trade Commission alleges we broke the law by sharing your health information without your permission. To resolve the case, we have agreed to an FTC order [\[notice will include link to the FTC.gov page with Complaint and Order\]](#) requiring that:

- We'll tell applicable third parties (like Facebook) who received that information to delete it.
- We'll never share your health information with applicable third parties (like Facebook) for advertising purposes.
- We won't share your health information with applicable third parties (like Facebook) for other purposes, unless we get your permission first.
- We'll put in place a comprehensive privacy program with heightened procedures and controls to protect your personal and health information. An independent auditor will review our program to make sure we're protecting your information. These audits will happen every two years for 20 years.

If you have any questions, email us at [privacy@goodrx.com](mailto:privacy@goodrx.com).

To learn more about the settlement, go to [ftc.gov](https://www.ftc.gov) and search for "GoodRx".

For advice on protecting your health privacy, read the FTC's [Does your health app protect your sensitive info?](#)



IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

**GOODRX HOLDINGS, INC.,** a corporation,  
also d/b/a GoodRx, GoodRx Gold, GoodRx  
Care, HeyDoctor, and HeyDoctor by  
GoodRx;

Defendant.

Case No. \_\_\_\_\_

**ACKNOWLEDGMENT BY  
AFFIDAVIT OF RECEIPT OF  
ORDER BY DEFENDANT [NAME]**

A. My name is \_\_\_\_\_, my job title is \_\_\_\_\_, and I am authorized to accept service of process on GoodRx Holdings, Inc. I am [a U.S. citizen] over the age of eighteen, and I have personal knowledge of the facts set forth in this Acknowledgment.

B. GoodRx Holdings, Inc., was a Defendant in U.S. v. GoodRx Holdings, Inc., et al., which is the court case listed near the top of this page.

C. On [\_\_\_\_\_, 202\_], I received a copy of the Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, which was signed by the Honorable [Judge's name] and entered by the Court on [Month \_\_, 202\_]. A true and correct copy of the Order that I received is attached to this Acknowledgment.

D. On [Month \_\_, 202\_], GoodRx Holdings, Inc., received a copy of the Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, which was signed by

the Honorable [*Judge's name*] and entered by the Court on [*Month* \_\_, 202\_]. The copy of the Order attached to this Acknowledgment is a true and correct copy of the Order it received.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on [*Month* \_\_, 202\_].

\_\_\_\_\_  
[*Full name*]  
Officer of  
GoodRx Holdings, Inc.

State of \_\_\_\_\_, City of \_\_\_\_\_

Subscribed and sworn to before me  
this \_\_\_\_ day of \_\_\_\_\_, 202\_\_.

\_\_\_\_\_  
Notary Public  
My commission expires:  
\_\_\_\_\_

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

**GOODRX HOLDINGS, INC.,** a corporation,  
also d/b/a GoodRx, GoodRx Gold, GoodRx  
Care, HeyDoctor, and HeyDoctor by  
GoodRx;

Defendant.

**Case No.** \_\_\_\_\_

**ACKNOWLEDGMENT BY  
DECLARATION OF RECEIPT OF  
ORDER BY A NON PARTY**

I, \_\_\_\_\_, received a copy of the Stipulated Order for  
Permanent Injunction, Civil Penalty Judgment, and Other Relief, in U.S. v. GoodRx Holdings,  
Inc., et al., on \_\_\_\_\_, 20\_\_.

I was not a Defendant in that court case. My title or relationship with Defendant  
is \_\_\_\_\_.

I declare under penalty of perjury under the laws of the United States of America that the  
foregoing is true and correct.

Executed on \_\_\_\_\_, 20\_\_.

Signed: \_\_\_\_\_

9

---

---

SENATE BILL NO. 370—SENATORS CANNIZZARO, NGUYEN,  
DONATE; DALY, D. HARRIS, LANGE, NEAL, PAZINA  
AND SCHEIBLE

MARCH 23, 2023

Referred to Committee on Commerce and Labor

SUMMARY—Revises provisions relating to consumer health data.  
(BDR 52-42)

FISCAL NOTE: Effect on Local Government: No.  
Effect on the State: Yes.

~

EXPLANATION – Matter in *bolded italics* is new; matter between brackets ~~omitted material~~ is material to be omitted.

---

---

AN ACT relating to data privacy; requiring certain entities to develop, maintain and make available on the Internet a policy concerning the privacy of consumer health data; prohibiting such an entity from collecting or sharing consumer health data without the affirmative consent of a consumer in certain circumstances; requiring such an entity to perform certain actions upon the request of a consumer; requiring such an entity to establish a process to appeal the denial of such a request; requiring such an entity to take certain actions to protect the security of consumer health data; limiting the circumstances under which a processor is authorized to process consumer health data; requiring a processor to assist certain entities in complying with certain requirements; prohibiting a person from selling or offering to sell consumer health data under certain circumstances; prohibiting the implementation of a geofence under certain circumstances; prohibiting discrimination against a consumer for certain reasons; authorizing certain civil actions; providing penalties; and providing other matters properly relating thereto.



**Legislative Counsel's Digest:**

1 Existing federal law and regulations contain various protections for health  
2 information maintained or used: (1) by a person or entity that provides health care,  
3 an insurer or a business associate of a person or entity that provides health care or  
4 an insurer; or (2) for scientific research. (42 U.S.C. §§ 11101 et seq.; Pub. L. No.  
5 104-191, 100 Stat. 2548; 21 C.F.R. Parts 46, 50 and 56, 42 C.F.R. Parts 2 and 3, 45  
6 C.F.R. Parts 160 and 164) This bill prescribes various protections for consumer  
7 health data that is maintained and used by other persons and nongovernmental  
8 entities and for other purposes. **Section 7** of this bill defines the term "consumer" to  
9 mean a natural person who resides in this State or whose consumer health data is  
10 collected in this State, except for a natural person acting in an employment context.  
11 **Section 8** of this bill defines the term "consumer health data" to mean personally  
12 identifiable information that is linked or reasonably capable of being linked to a  
13 consumer and is related to the health of the consumer. **Section 15** of this bill  
14 defines the term "regulated entity" to refer to a person who: (1) conducts business  
15 in this State or produces or provides products or services that are targeted to  
16 consumers in this State; and (2) determines the purpose and means of processing,  
17 sharing or selling consumer health data. **Sections 3-6, 9-14 and 16-19** of this bill  
18 define certain other terms. **Section 20** of this bill provides that the provisions of this  
19 bill do not apply to certain data that is collected or disclosed under certain  
20 provisions of federal law or regulations or state law.

21 **Section 21** of this bill requires a regulated entity to develop, maintain and make  
22 available on the Internet a policy concerning the privacy of consumer health data.  
23 **Section 21** also prohibits a regulated entity from: (1) taking certain actions with  
24 regard to consumer health data that are inconsistent with the policy without the  
25 affirmative consent of the consumer; or (2) entering into a contract for the  
26 processing of consumer health data that is inconsistent with the policy. **Section 22**  
27 of this bill generally prohibits a regulated entity from collecting or sharing  
28 consumer health data without the affirmative consent of the consumer to whom the  
29 data relates, except to the extent necessary to provide a product or service that the  
30 consumer has requested from the regulated entity. **Sections 22 and 23** of this bill  
31 prescribe certain requirements governing such consent.

32 **Section 24** of this bill requires a regulated entity, upon the request of a  
33 consumer, to: (1) confirm whether the regulated entity is collecting, sharing or  
34 selling consumer health data concerning the consumer; (2) provide the consumer  
35 with a list of all third parties and affiliates with whom the regulated entity has  
36 shared or to whom the regulated entity has sold consumer health data relating to the  
37 consumer; (3) cease collecting or sharing consumer health data relating to the  
38 consumer; or (4) delete consumer health data concerning the consumer. **Section 24**  
39 also requires a regulated entity to establish a secure and reliable means of making  
40 such a request. **Section 25** of this bill prescribes requirements governing the  
41 response to such a request, including a requirement that a regulated entity provide  
42 information in response to such a request free of charge in most circumstances.  
43 However, if a consumer submits more than two requests in a year and those  
44 requests are manifestly unfounded, excessive or repetitive, **section 25** authorizes  
45 the regulated entity to charge a reasonable fee to provide such information. **Section**  
46 **26** of this bill prescribes requirements governing the time within which a regulated  
47 entity or an affiliate, processor or other third party with which a regulated entity has  
48 shared data must delete consumer health data in response to a request for such  
49 deletion. **Section 27** of this bill requires a regulated entity to establish a process to  
50 appeal the refusal of the regulated entity to act on a request made pursuant to  
51 **section 24**. **Section 32** of this bill: (1) requires a regulated entity, contractor of a  
52 regulated entity, processor or other third party to disclose consumer health data  
53 where required by law, court order, subpoena or search warrant; (2) authorizes  
54 certain other disclosures of consumer health data; and (3) provides that a regulated



entity, contractor, processor or third party who discloses consumer health data under such circumstances is not required to comply with **sections 22-27**.

**Section 28** of this bill requires a regulated entity to limit access to and establish, implement and maintain policies and procedures to protect the security of consumer health data. **Section 29** of this bill requires a processor who processes consumer health data on behalf of a regulated entity to only process such data in accordance with a written contract between the processor and the regulated entity. **Section 29** also requires such a processor to assist a regulated entity in complying with the provisions of this bill.

**Section 30** of this bill prohibits a person from selling or offering to sell consumer health data without the written authorization of the consumer to whom the data pertains or beyond the scope of such authorization, with certain exceptions. **Section 30** also prohibits a person from conditioning the provision of goods or services on a consumer providing such authorization. **Section 30** requires a person who sells consumer health data to: (1) establish a means by which a consumer may revoke such written authorization; and (2) provide a copy of such written authorization to the consumer. **Section 30** also requires both a seller and a purchaser of consumer health data to maintain such written authorization for at least 6 years after the expiration of the written authorization.

**Section 31** of this bill prohibits a person from implementing a geofence around any person or entity that provides in-person health care services or products for certain purposes. **Section 33** of this bill prohibits a regulated entity from discriminating against a consumer for taking any action authorized by this bill or to enforce the provisions of this bill.

Existing law provides that a variety of actions constitute deceptive trade practices. (NRS 118A.275, 205.377, 228.620, 370.695, 597.997, 603.170, 604B.910, 676A.770; chapter 598 of NRS) Existing law authorizes a court to impose a civil penalty of not more than \$12,500 for each violation upon a person whom the court finds has engaged in a deceptive trade practice directed toward an elderly person or a person with a disability. (NRS 598.0973) Additionally, existing law authorizes a court to make such additional orders or judgments as may be necessary to restore to any person in interest any money or property which may have been acquired by means of any deceptive trade practice. (NRS 598.0993) In addition to these enforcement mechanisms, existing law provides that when the Commissioner of Consumer Affairs or the Director of the Department of Business and Industry has cause to believe that a person has engaged or is engaging in any deceptive trade practice, the Commissioner or Director may request that the Attorney General represent him or her in instituting an appropriate legal proceeding, including an application for an injunction or temporary restraining order. (NRS 598.0979) Existing law provides that if a person violates a court order or injunction resulting from a complaint brought by the Commissioner, the Director, the district attorney of any county of this State or the Attorney General, the person is required to pay a civil penalty of not more than \$10,000 for each violation. Furthermore, if a court finds that a person has willfully engaged in a deceptive trade practice, the person who committed the violation: (1) may be required to pay an additional civil penalty not more than \$5,000 for each violation; and (2) is guilty of a felony or misdemeanor, depending on the value of the property or services lost as a result of the deceptive trade practice. (NRS 598.0999) Existing law: (1) provides that certain deceptive trade practices constitute consumer fraud; and (2) authorizes a person injured by consumer fraud to bring a civil action. (NRS 41.600) With certain exceptions, **section 34** of this bill: (1) provides that a person who violates any provision of this bill is guilty of a deceptive trade practice; and (2) authorizes a person injured by such a violation to bring a civil action.

**Section 35** of this bill exempts consumer health data from provisions of existing



109 law governing information collected on the Internet from consumers because those  
110 provisions are less stringent than the provisions of **sections 2-34** of this bill.

---

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN  
SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

1     **Section 1.** Chapter 603A of NRS is hereby amended by  
2 adding thereto the provisions set forth as sections 2 to 34, inclusive,  
3 of this act.

4     **Sec. 2.** *As used in sections 2 to 34, inclusive, of this act,*  
5 *unless the context otherwise requires, the words and terms defined*  
6 *in sections 3 to 19, inclusive, of this act have the meanings*  
7 *ascribed to them in those sections.*

8     **Sec. 3.** *“Affiliate” means an entity that shares common*  
9 *branding with another entity and controls, is controlled by or is*  
10 *under common control with the other entity. For the purposes of*  
11 *this section, an entity shall be deemed to control another entity if*  
12 *the entity:*

13         1. *Owns or has the power to vote at least half of the*  
14 *outstanding shares of any class of voting security in the other*  
15 *entity;*

16         2. *Controls in any manner the election of a majority of the*  
17 *directors or persons exercising similar functions to directors of the*  
18 *other entity; or*

19         3. *Has the power to exercise controlling influence over the*  
20 *management of the other entity.*

21     **Sec. 4.** *“Authenticate” means to ascertain the identity of the*  
22 *originator of an electronic or physical document and establish a*  
23 *link between the document and the originator.*

24     **Sec. 5.** *“Biometric data” means data which is generated from*  
25 *the measurement or technical processing of the physiological,*  
26 *biological or behavioral characteristics of a person and, alone or*  
27 *in combination with other data, is capable of being used to identify*  
28 *the person. The term includes, without limitation:*

29         1. *Imagery of the fingerprint, palm print, hand print, scar,*  
30 *bodily mark, tattoo, voiceprint, face, retina, iris or vein pattern of a*  
31 *person; and*

32         2. *Keystroke patterns or rhythms and gait patterns or rhythms*  
33 *that contain identifying information.*

34     **Sec. 6.** *“Collect” means to buy, rent, access, retain, receive,*  
35 *acquire, infer, derive or otherwise process consumer health data*  
36 *in any manner.*

37     **Sec. 7.** *“Consumer” means a natural person who resides in*  
38 *this State or whose consumer health data is collected in this State.*





1 *The term does not include a natural person acting in an*  
2 *employment context.*

3 **Sec. 8.** *“Consumer health data” means personally*  
4 *identifiable information that is linked or reasonably capable of*  
5 *being linked to a consumer and is related to the past, present or*  
6 *future health of the consumer. The term includes, without*  
7 *limitation:*

8 1. *Information relating to:*

9 (a) *Any health condition or status, disease or diagnosis;*

10 (b) *Social, psychological, behavioral or medical interventions;*

11 (c) *Surgeries or other health-related procedures;*

12 (d) *The use or acquisition of medication;*

13 (e) *Bodily functions, vital signs or symptoms;*

14 (f) *Reproductive or sexual health care; and*

15 (g) *Gender-affirming care;*

16 2. *Biometric data or genetic data related to information*  
17 *described in subsection I;*

18 3. *Information related to the precise location of a consumer*  
19 *that is derived from technology, including, without limitation, a*  
20 *global positioning system, and is reasonably capable of being used*  
21 *to indicate an attempt by a consumer to receive health care*  
22 *services or products; and*

23 4. *Any information described in subsection 1, 2 or 3 that is*  
24 *derived or extrapolated from information that is not consumer*  
25 *health data, including, without limitation, proxy, derivative,*  
26 *inferred or emergent data derived through an algorithm, machine*  
27 *learning or any other means.*

28 **Sec. 9.** *“Gender-affirming care” means health services or*  
29 *products that support and affirm the gender identity of a person,*  
30 *including, without limitation:*

31 1. *Treatments for gender dysphoria;*

32 2. *Gender-affirming hormone therapy; and*

33 3. *Gender-affirming surgery.*

34 **Sec. 10.** *“Genetic data” means any data that concerns the*  
35 *genetic characteristics of a person. The term includes, without*  
36 *limitation:*

37 1. *Data directly resulting from the sequencing of all or a*  
38 *portion of the deoxyribonucleic acid of a person;*

39 2. *Genotypic and phenotypic information that results from*  
40 *analyzing the information described in subsection I; and*

41 3. *Data concerning the health of a person that is analyzed in*  
42 *connection with the information described in subsection I.*

43 **Sec. 11.** *“Health care services or products” means any*  
44 *service or product provided to a person to assess, measure,*



1 *improve or learn about the health of a person. The term includes,*  
2 *without limitation:*

3 1. *Services relating to any health condition or status, disease*  
4 *or diagnosis;*

5 2. *Social, psychological, behavioral or medical interventions;*

6 3. *Surgeries or other health-related procedures;*

7 4. *Medication or services related to the use or acquisition of*  
8 *medication; or*

9 5. *Monitoring or measurement related to bodily functions,*  
10 *vital signs or symptoms.*

11 **Sec. 12.** *“Personally identifiable information” means*  
12 *information that, alone or in combination with other information,*  
13 *may be used to identify a person or an electronic device used by*  
14 *the person. The term:*

15 1. *Includes, without limitation:*

16 (a) *Data associated with an Internet protocol address, device*  
17 *identifier or other form of persistent unique identifier; and*

18 (b) *Any data about a person that is collected without the*  
19 *consent of the person.*

20 2. *Does not include:*

21 (a) *Information that is made lawfully available through the*  
22 *records of a federal, state or local governmental entity or widely*  
23 *distributed media and which a regulated entity has a reasonable*  
24 *basis to believe that a person has made available to the general*  
25 *public; or*

26 (b) *Deidentified information.*

27 **Sec. 13.** *“Process” means any operation or set of operations*  
28 *performed on consumer health data.*

29 **Sec. 14.** *“Processor” means a person who processes*  
30 *consumer health data on behalf of a regulated entity.*

31 **Sec. 15.** *“Regulated entity” means any person who:*

32 1. *Conducts business in this State or produces or provides*  
33 *products or services that are targeted to consumers in this State;*  
34 *and*

35 2. *Alone or with other persons, determines the purpose and*  
36 *means of processing, sharing or selling consumer health data.*

37 **Sec. 16.** *“Reproductive or sexual health care” means health*  
38 *care services or products that support or relate to the reproductive*  
39 *system or sexual well-being of a person. The term includes,*  
40 *without limitation, abortion, the provision of medication to induce*  
41 *an abortion and any medical or nonmedical services associated*  
42 *with an abortion.*

43 **Sec. 17.** *“Sell” means to exchange consumer health*  
44 *information for money or other valuable consideration.*



1     **Sec. 18.** *“Share” means to release, disclose, disseminate,*  
2 *divulge, make available, provide access to, license or otherwise*  
3 *communicate consumer health data orally, in writing or by*  
4 *electronic or other means.*

5     **Sec. 19.** *“Third party” means a person who is not a*  
6 *consumer, regulated entity, processor or affiliate of a regulated*  
7 *entity.*

8     **Sec. 20.** *The provisions of sections 2 to 34, inclusive, of this*  
9 *act do not apply to:*

10     1. *Information that is collected, used or shared in accordance*  
11 *with the Health Insurance Portability and Accountability Act of*  
12 *1996, Public Law 104-191, and the regulations adopted pursuant*  
13 *thereto.*

14     2. *Information originating from, and intermingled with to be*  
15 *indistinguishable from, information described in subsection 1 that*  
16 *is maintained by:*

17         (a) *A covered entity or business associate, as those terms are*  
18 *defined in 45 C.F.R. § 160.103; or*

19         (b) *A program or qualified service organization, as those terms*  
20 *are defined in 45 C.F.R. § 2.11.*

21     3. *Patient identifying information, as defined in 42 C.F.R. §*  
22 *2.11, that is collected, used or disclosed in accordance with 42*  
23 *C.F.R. Part 2.*

24     4. *Patient safety work product, as defined in 42 C.F.R. § 3.20,*  
25 *that is collected, used or disclosed in accordance with 42 C.F.R.*  
26 *Part 3.*

27     5. *Identifiable private information, as defined in 45 C.F.R. §*  
28 *46.102, that is collected, used or disclosed in accordance with 45*  
29 *C.F.R. Part 46.*

30     6. *Information used or shared as part of research conducted*  
31 *pursuant to 45 C.F.R. Part 46 or 21 C.F.R. Parts 50 and 56.*

32     7. *Information used only for public health activities and*  
33 *purposes, as described in 45 C.F.R. § 164.512(b), regardless of*  
34 *whether such information is subject to the Health Insurance*  
35 *Portability and Accountability Act of 1996, Public Law 104-191,*  
36 *and the regulations adopted pursuant thereto.*

37     8. *Personally identifiable information that is governed by and*  
38 *collected, used or disclosed pursuant to:*

39         (a) *The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq.,*  
40 *and the regulations adopted pursuant thereto;*

41         (b) *Part C of Title XI of the Social Security Act, 42 U.S.C. §§*  
42 *1320d et seq.;*

43         (c) *The Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq.;*  
44 *or*



1 *(d) The Family Educational Rights and Privacy Act of 1974,*  
2 *20 U.S.C. § 1232g, and the regulations adopted pursuant thereto.*

3 *9. Information and documents created for the purposes of*  
4 *compliance with the federal Health Care Quality Improvement Act*  
5 *of 1986, 42 U.S.C. §§ 11101 et seq., and any regulations adopted*  
6 *pursuant thereto.*

7 *10. The collection or sharing of consumer health data where*  
8 *expressly authorized by any provision of state law.*

9 *11. Any governmental or tribal entity or any person*  
10 *processing consumer health data on behalf of a governmental or*  
11 *tribal entity.*

12 **Sec. 21. 1. A regulated entity shall develop and maintain a**  
13 **policy concerning the privacy of consumer health data that clearly**  
14 **and conspicuously establishes:**

15 *(a) The categories of consumer health data being collected by*  
16 *the regulated entity and the manner in which the consumer health*  
17 *data will be used;*

18 *(b) The categories of sources from which consumer health*  
19 *data is collected;*

20 *(c) The categories of consumer health data that are shared by*  
21 *the regulated entity;*

22 *(d) A list of third parties and affiliates with whom the*  
23 *regulated entity shares consumer health data;*

24 *(e) The purposes of collecting, using and sharing consumer*  
25 *health data;*

26 *(f) The manner in which consumer health data will be*  
27 *processed;*

28 *(g) The procedure for submitting a request pursuant to section*  
29 *24 of this act;*

30 *(h) The process, if any such process exists, for a consumer to*  
31 *review and request changes to any of his or her consumer health*  
32 *data that is collected by the regulated entity;*

33 *(i) The process by which the regulated entity notifies*  
34 *consumers whose consumer health data is collected by the*  
35 *regulated entity of material changes to the privacy policy;*

36 *(j) Whether a third party may collect consumer health data*  
37 *over time and across different Internet websites or online services*  
38 *when the consumer uses any Internet website or online service of*  
39 *the regulated entity; and*

40 *(k) The effective date of the privacy policy.*

41 **2. A regulated entity shall post conspicuously on the main**  
42 **Internet website maintained by the regulated entity a hyperlink to**  
43 **the policy developed pursuant to subsection 1.**

44 **3. A regulated entity shall not:**



1 (a) *Collect, use or share categories of consumer health data,*  
2 *other than those included in the privacy policy pursuant to*  
3 *paragraph (c) of subsection 1, without disclosing those additional*  
4 *categories to each consumer whose data will be collected, used or*  
5 *shared and obtaining the affirmative consent of the consumer;*

6 (b) *Share consumer health data with a third party or affiliate,*  
7 *other than those included in the privacy policy pursuant to*  
8 *paragraph (d) of subsection 1, without disclosing those additional*  
9 *third parties or affiliates to each consumer whose data will be*  
10 *shared and obtaining the affirmative consent of the consumer;*

11 (c) *Collect, use or share consumer health data for purposes*  
12 *other than those included in the privacy policy pursuant to*  
13 *paragraph (e) of subsection 1 without disclosing those additional*  
14 *purposes to each consumer whose data will be collected, used or*  
15 *shared and obtaining the affirmative consent of the consumer; or*

16 (d) *Enter into a contract pursuant to section 29 of this act with*  
17 *a processor to process consumer health data that is inconsistent*  
18 *with the privacy policy.*

19 **Sec. 22. 1.** *A regulated entity shall not collect consumer*  
20 *health data except:*

21 (a) *With the affirmative consent of the consumer; or*

22 (b) *To the extent necessary to provide a product or service that*  
23 *the consumer to whom the consumer health data relates has*  
24 *requested from the regulated entity.*

25 **2.** *A regulated entity shall not share consumer health data*  
26 *except:*

27 (a) *With the affirmative consent of the consumer to whom the*  
28 *consumer health data relates, which must be separate and distinct*  
29 *from the consent provided pursuant to subsection 1 for the*  
30 *collection of the data;*

31 (b) *To the extent necessary to provide a product or service that*  
32 *the consumer to whom the consumer health data relates has*  
33 *requested from the regulated entity; or*

34 (c) *Where required or authorized by section 32 of this act.*

35 **3.** *Any consent required by this section must be obtained*  
36 *before the collection or sharing, as applicable, of consumer health*  
37 *data. The request for such consent must clearly and conspicuously*  
38 *disclose:*

39 (a) *The categories of consumer health data to be collected or*  
40 *shared, as applicable;*

41 (b) *The purpose for collecting or sharing, as applicable, the*  
42 *consumer health data including, without limitation, the manner in*  
43 *which the consumer health data will be used;*



1 (c) *If the consumer health data will be shared, the categories*  
2 *of persons and entities with whom the consumer health data will*  
3 *be shared; and*

4 (d) *The manner in which the consumer may withdraw consent*  
5 *for the collection or sharing, as applicable, of consumer health*  
6 *data relating to the consumer and request that the regulated entity*  
7 *cease such collection or sharing pursuant to section 24 of this act.*

8 **Sec. 23.** *Any consent provided pursuant to section 21 or 22 of*  
9 *this act must be an affirmative, voluntary act. Such consent may*  
10 *be provided electronically, but may not be provided through:*

11 1. *The acceptance of a general agreement concerning terms*  
12 *of use or a similar agreement that contains descriptions of the*  
13 *manner in which personal data will be used or processed and*  
14 *other unrelated information;*

15 2. *A consumer hovering over, muting, pausing or closing a*  
16 *piece of online content; or*

17 3. *The use of a user interface designed or manipulated with*  
18 *the effect of subverting or impairing the autonomy, decision*  
19 *making or choice of the user.*

20 **Sec. 24.** 1. *Except as otherwise provided in section 25 of*  
21 *this act, upon the request of a consumer, a regulated entity shall:*

22 (a) *Confirm whether the regulated entity is collecting, sharing*  
23 *or selling consumer health data relating to the consumer.*

24 (b) *Provide the consumer with a list of all third parties and*  
25 *affiliates with whom the regulated entity has shared consumer*  
26 *health data relating to the consumer or to whom the regulated*  
27 *entity has sold such consumer health data. The list must include,*  
28 *without limitation, a valid electronic mail address for each such*  
29 *third party or affiliate or another valid mechanism by which the*  
30 *consumer may contact each such third party or affiliate using the*  
31 *Internet.*

32 (c) *Cease collecting, sharing or selling consumer health data*  
33 *relating to the consumer.*

34 (d) *Delete consumer health data concerning the consumer.*

35 2. *A regulated entity shall establish a secure and reliable*  
36 *means of making a request pursuant to this section. The means of*  
37 *making such a request must not require a consumer to create a*  
38 *new account with the regulated entity, but may require the*  
39 *consumer to use an existing account. When establishing the*  
40 *means for making such a request, the regulated entity must*  
41 *consider:*

42 (a) *The need for the safe and reliable communication of such*  
43 *requests; and*

44 (b) *The ability of the regulated entity to authenticate the*  
45 *identity of the consumer making the request.*



1     **Sec. 25. 1.** *Except as otherwise provided in this section, a*  
2 *regulated entity shall respond to a request made pursuant to*  
3 *section 24 of this act without undue delay and not later than 45*  
4 *days after authenticating the request. If reasonably necessary*  
5 *based on the complexity and number of requests from the same*  
6 *consumer, the regulated entity may extend the period prescribed*  
7 *by this section not more than an additional 45 days. A regulated*  
8 *entity that grants itself such an extension must, not later than 45*  
9 *days after authenticating the request, provide the consumer with*  
10 *notice of the extension and the reasons therefor.*

11     **2.** *If a regulated entity is not able to authenticate a request*  
12 *made pursuant to section 24 of this act after making commercially*  
13 *reasonable efforts, the regulated entity:*

14         **(a)** *Is not required to comply with the request; and*

15         **(b)** *May request that the consumer provide such additional*  
16 *information as is reasonably necessary to authenticate the request.*

17     **3.** *A regulated entity:*

18         **(a)** *Shall provide information free of charge to a consumer in*  
19 *response to:*

20             **(1)** *Requests made pursuant to section 24 of this act at least*  
21 *twice each year; and*

22             **(2)** *Additional requests that are not manifestly unfounded,*  
23 *excessive or repetitive.*

24         **(b)** *Except as otherwise provided in paragraph (a), may charge*  
25 *a reasonable fee to provide information to a consumer in response*  
26 *to requests made pursuant to section 24 of this act that are*  
27 *manifestly unfounded, excessive or repetitive.*

28     **4.** *In any civil proceeding challenging the validity of a fee*  
29 *charged pursuant to paragraph (b) of subsection 3, the regulated*  
30 *entity has the burden of demonstrating by a preponderance of the*  
31 *evidence that the request to which the fee pertained was manifestly*  
32 *unfounded, excessive or repetitive.*

33     **5.** *In any criminal proceeding to enforce the provisions of*  
34 *this section, it is an affirmative defense that the regulated entity*  
35 *charged a fee pursuant to paragraph (b) of subsection 3 in*  
36 *response to a request that was manifestly unfounded, excessive or*  
37 *repetitive.*

38     **Sec. 26. 1.** *Not later than 30 days after authenticating a*  
39 *request made pursuant to paragraph (d) of subsection 1 of section*  
40 *24 of this act for the deletion of consumer health data, a regulated*  
41 *entity shall, except as otherwise provided in subsection 3:*

42         **(a)** *Delete all consumer health data described in the request*  
43 *from the records and network of the regulated entity; and*



1 (b) Notify each affiliate, processor, contractor or other third  
2 party with which the regulated entity has shared consumer health  
3 data of the deletion request.

4 2. Not later than 30 days after receiving notification of a  
5 deletion request pursuant to paragraph (b) of subsection 1, an  
6 affiliate, processor, contractor or other third party shall, except as  
7 otherwise provided in subsection 3, delete the consumer health  
8 data described in the request from the records and network of the  
9 affiliate, processor, contractor or other third party.

10 3. If data described in a deletion request made pursuant to  
11 paragraph (d) of subsection 1 of section 24 of this act is stored or  
12 archived on backup systems, a regulated entity or an affiliate,  
13 processor, contractor or other third party may delay the deletion of  
14 the data for not more than 6 months after the request is  
15 authenticated, as necessary to restore the archived or backup  
16 system.

17 **Sec. 27. 1.** A regulated entity shall establish a process by  
18 which a consumer may appeal the refusal of the regulated entity to  
19 act on a request made pursuant section 24 of this act. The process  
20 must be:

21 (a) Conspicuously available on the Internet website of the  
22 regulated entity; and

23 (b) Similar to the process for making a request pursuant to  
24 section 24 of this act.

25 2. Not later than 45 days after receiving an appeal pursuant  
26 to subsection 1, a regulated entity shall inform the consumer in  
27 writing of:

28 (a) Any action taken in response to the appeal or any decision  
29 not to take such action;

30 (b) The reasons for any such action or decision; and

31 (c) If the regulated entity decided not to take the action  
32 requested in the appeal, the contact information for the Office of  
33 the Attorney General.

34 **Sec. 28. 1.** A regulated entity shall only authorize the  
35 employees, processors and contractors of the regulated entity to  
36 access consumer health data where necessary to:

37 (a) Further the purpose for which the consumer consented to  
38 the collection or sharing of the consumer data pursuant to section  
39 22 of this act; or

40 (b) Provide a product or service that the consumer to whom  
41 the consumer health data relates has requested from the regulated  
42 entity.

43 2. A regulated entity shall establish, implement and maintain  
44 policies and practices for the administrative, technical and  
45 physical security of consumer health data. The policies must:





1 (a) Satisfy the standard of care in the industry in which the  
2 regulated entity operates to protect the confidentiality, integrity  
3 and accessibility of consumer health data;

4 (b) Comply with the provisions of NRS 603A.010 to 603A.290,  
5 inclusive, where applicable; and

6 (c) Be reasonable, taking into account the volume and nature  
7 of the consumer health data at issue.

8 **Sec. 29. 1.** A processor shall only process consumer health  
9 data pursuant to a contract between the processor and a regulated  
10 entity. Such a contract must set forth the applicable processing  
11 instructions and the specific actions that the processor is  
12 authorized to take with regard to the consumer health data it  
13 possesses on behalf of the regulated entity.

14 2. To the extent practicable, a processor shall assist a  
15 regulated entity with which the processor has entered into a  
16 contract pursuant to subsection 1 in complying with the provisions  
17 of sections 2 to 34, inclusive, of this act.

18 3. If a processor processes consumer health data outside the  
19 scope of a contract described in subsection 1 or in a manner  
20 inconsistent with any provision of such a contract, the processor:

21 (a) Is not guilty of an unfair trade practice or subject to a civil  
22 action pursuant to section 34 of this act solely because the  
23 processor violated the requirements of this section; and

24 (b) Shall be deemed a regulated entity for the purposes of  
25 sections 2 to 34, inclusive, of this act.

26 **Sec. 30. 1.** A person shall not sell or offer to sell consumer  
27 health data:

28 (a) Without the written authorization of the consumer to whom  
29 the data pertains; or

30 (b) If the consumer provides such written authorization, in a  
31 manner that is outside the scope of or inconsistent with the written  
32 authorization.

33 2. A person shall not condition the provision of goods or  
34 services on a consumer authorizing the sale of consumer health  
35 data pursuant to subsection 1.

36 3. Written authorization pursuant to subsection 1 must be  
37 provided in a form written in plain language which includes,  
38 without limitation:

39 (a) The name and contact information of the person selling the  
40 consumer health data;

41 (b) A description of the specific consumer health data that the  
42 person intends to sell;

43 (c) The name and contact information of the person  
44 purchasing the consumer health data;



1 (d) A description of the purpose of the sale, including, without  
2 limitation, the manner in which the consumer health data will be  
3 gathered and the manner in which the person described in  
4 paragraph (c) intends to use the consumer health data;

5 (e) A statement of the provisions of subsection 2;

6 (f) A statement that the consumer may revoke the written  
7 authorization at any time and a description of the means  
8 established pursuant to subsection 4 for revoking the  
9 authorization;

10 (g) A statement that any consumer health data sold pursuant  
11 to the written authorization may be disclosed to additional persons  
12 and entities by the person described in paragraph (c) and, after  
13 such disclosure, is no longer subject to the protections of this  
14 section;

15 (h) The date on which the written authorization expires  
16 pursuant to subsection 5; and

17 (i) The signature of the consumer to which the consumer  
18 health data pertains.

19 4. A person who sells consumer health data shall establish a  
20 means by which a consumer may revoke a written authorization  
21 made pursuant to subsection 1.

22 5. Written authorization provided pursuant to subsection 1  
23 expires 1 year after the date on which the authorization is given.

24 6. A written authorization provided pursuant to subsection 1  
25 is not valid if the written authorization:

26 (a) Was a condition for the provision of goods or services to  
27 the consumer in violation of subsection 2;

28 (b) Does not comply with the requirements of subsection 3;

29 (c) Has been revoked pursuant to subsection 4; or

30 (d) Has expired pursuant to subsection 5.

31 7. A person who sells consumer health data shall provide a  
32 copy of the written authorization provided pursuant to subsection  
33 1 to the consumer who signed the written authorization.

34 8. A seller and purchaser of consumer health data shall each  
35 retain a copy of the written authorization provided pursuant to  
36 subsection 1 for at least 6 years after the date on which the written  
37 authorization expired pursuant to subsection 5.

38 9. The provisions of this section do not apply to the sale of  
39 consumer health data to:

40 (a) A processor in a manner consistent with the purpose for  
41 which the consumer health data was collected, as disclosed to the  
42 consumer to whom the consumer health data pertains pursuant to  
43 section 22 of this act; or

44 (b) A third party as an asset that is part of a merger,  
45 acquisition, bankruptcy or other transaction through which the



1 *third party assumes control of all or part of the assets of the*  
2 *regulated entity. A third party that obtains consumer health data*  
3 *from a regulated entity pursuant to this paragraph assumes all*  
4 *obligations of the regulated entity to comply with the provisions of*  
5 *sections 2 to 34, inclusive, of this act.*

6 **Sec. 31.** 1. *A person shall not implement a geofence within*  
7 *2,000 feet of any medical facility, facility for the dependent or any*  
8 *other person or entity that provides in-person health care services*  
9 *or products for the purpose of:*

10 (a) *Identifying or tracking consumers seeking in-person health*  
11 *care services or products;*

12 (b) *Collecting consumer health data; or*

13 (c) *Sending notifications, messages or advertisements to*  
14 *consumers related to their consumer health data or health care*  
15 *services or products.*

16 2. *As used in this section:*

17 (a) *“Facility for the dependent” has the meaning ascribed to it*  
18 *in NRS 449.0045.*

19 (b) *“Geofence” means technology that uses coordinates for*  
20 *global positioning, connectivity to cellular towers, cellular data,*  
21 *radio frequency identification, wireless Internet data or any other*  
22 *form of detecting the physical location of a person to establish a*  
23 *virtual boundary around a specific physical location.*

24 (c) *“Medical facility” has the meaning ascribed to it in*  
25 *NRS 449.0151.*

26 **Sec. 32.** 1. *A regulated entity, contractor of a regulated*  
27 *entity, processor or other third party that is in possession of*  
28 *consumer health data:*

29 (a) *Shall disclose the consumer health data where required by*  
30 *law, a court order, a subpoena, a search warrant or other lawful*  
31 *process; and*

32 (b) *Is not required to comply with the provisions of sections 22*  
33 *to 27, inclusive, of this act, when making such a disclosure.*

34 2. *A regulated entity may share consumer health data without*  
35 *complying with the provisions of sections 22 to 27, inclusive, of*  
36 *this act:*

37 (a) *Directly with a processor for the purpose of providing*  
38 *goods or services in a manner consistent with the purpose for*  
39 *which the consumer health data was collected, as disclosed to the*  
40 *consumer to whom the consumer health data pertains pursuant to*  
41 *section 22 of this act.*

42 (b) *With a third party with whom the consumer to whom the*  
43 *consumer health data relates has a direct relationship if:*

44 (1) *The disclosure is for the purpose of providing a product*  
45 *or service requested by the consumer;*



1           (2) *The regulated entity maintains control and ownership*  
2 *of the consumer health data; and*

3           (3) *The third party uses the consumer health data as*  
4 *directed by the regulated entity and in a manner consistent with*  
5 *the purpose for which the consumer health data was collected, as*  
6 *disclosed to the consumer to whom the consumer health data*  
7 *relates pursuant to section 22 of this act.*

8           (c) *With a third party as an asset that is part of a merger,*  
9 *acquisition, bankruptcy or other transaction through which the*  
10 *third party assumes control of all or part of the assets of the*  
11 *regulated entity. A third party that obtains consumer health data*  
12 *from a regulated entity pursuant to this paragraph assumes all*  
13 *obligations of the regulated entity to comply with the provisions of*  
14 *sections 2 to 34, inclusive, of this act.*

15           3. *A regulated entity or processor may collect, use or disclose*  
16 *consumer health data without complying with the provisions of*  
17 *sections 22 to 27, inclusive, of this act to:*

18           (a) *Prevent, detect, protect against, respond to, investigate,*  
19 *report or aid in the prosecution of malicious, deceptive or illegal*  
20 *activities, security incidents, identity theft, fraud or harassment; or*

21           (b) *Preserve the integrity or security of electronic systems.*

22           4. *In any civil proceeding where a regulated entity or*  
23 *processor is alleged to have failed to comply with the provisions of*  
24 *sections 22 to 27, inclusive, of this act, a regulated entity or*  
25 *processor that collected, used or disclosed the consumer health*  
26 *data for a purpose described in subsection 3 has the burden of*  
27 *demonstrating by a preponderance of the evidence that the*  
28 *collection, use or disclosure was for such a purpose.*

29           5. *In any criminal proceeding where a regulated entity or*  
30 *processor is alleged to have failed to comply with the provisions of*  
31 *sections 22 to 27, inclusive, of this act, it is an affirmative defense*  
32 *that a regulated entity or processor collected, used or disclosed*  
33 *consumer health data for a purpose described in subsection 3.*

34           **Sec. 33.** *A regulated entity shall not discriminate against a*  
35 *consumer for taking:*

36           1. *Any action authorized by sections 2 to 34, inclusive, of this*  
37 *act; or*

38           2. *Any action to enforce the provisions of sections 2 to 34,*  
39 *inclusive, of this act.*

40           **Sec. 34.** 1. *Except as otherwise provided in section 29 of*  
41 *this act:*

42           (a) *A violation of sections 2 to 34, inclusive, of this act*  
43 *constitutes a deceptive trade practice for the purposes of NRS*  
44 *598.0903 to 598.0999, inclusive.*



1       ***(b) An action may be brought by any person who is a victim of***  
2 ***a violation of sections 2 to 34, inclusive, of this act. If the claimant***  
3 ***is the prevailing party, the court shall award the claimant:***

4           ***(1) Any damages that the claimant has sustained;***

5           ***(2) Any equitable relief that the court deems appropriate;***  
6 ***and***

7           ***(3) The claimant's costs in the action and reasonable***  
8 ***attorney's fees.***

9       ***2. Any action brought pursuant to this section is not an***  
10 ***action upon any contract underlying the original transaction.***

11       **Sec. 35.** NRS 603A.338 is hereby amended to read as follows:

12       603A.338 The provisions of NRS 603A.300 to 603A.360,  
13 inclusive, do not apply to:

14       1. A consumer reporting agency, as defined in 15 U.S.C. §  
15 1681a(f);

16       2. Any personally identifiable information regulated by the  
17 Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq., and the  
18 regulations adopted pursuant thereto, which is collected, maintained or  
19 sold as provided in that Act;

20       3. A person who collects, maintains or makes sales of  
21 personally identifiable information for the purposes of fraud  
22 prevention;

23       4. Any personally identifiable information that is publicly  
24 available;

25       5. Any personally identifiable information protected from  
26 disclosure under the federal Driver's Privacy Protection Act of  
27 1994, 18 U.S.C. §§ 2721 et seq., which is collected, maintained or  
28 sold as provided in that Act; ~~or~~

29       6. ***Any consumer health data subject to the provisions of***  
30 ***sections 2 to 34, inclusive, of this act; or***

31       7. A financial institution or an affiliate of a financial institution  
32 that is subject to the provisions of the Gramm-Leach-Bliley Act, 15  
33 U.S.C. §§ 6801 et seq., or any personally identifiable information  
34 regulated by that Act which is collected, maintained or sold as  
35 provided in that Act.



10

## Chapter 12: Biometric Identifier Information

### § 22-1201 Definitions.

As used in this chapter, the following terms have the following meanings:

**Biometric identifier information.** The term "biometric identifier information" means a physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic.

**Commercial establishment.** The term "commercial establishment" means a place of entertainment, a retail store, or a food and drink establishment.

**Consumer commodity.** The term "consumer commodity" means any article, good, merchandise, product or commodity of any kind or class produced, distributed or offered for retail sale for consumption by individuals, or for personal, household or family purposes.

**Customer.** The term "customer" means a purchaser or lessee, or a prospective purchaser or lessee, of goods or services from a commercial establishment.

**Financial institution.** The term "financial institution" means a bank, trust company, national bank, savings bank, federal mutual savings bank, savings and loan association, federal savings and loan association, federal mutual savings and loan association, credit union, federal credit union, branch of a foreign banking corporation, public pension fund, retirement system, securities broker, securities dealer or securities firm, but does not include a commercial establishment whose primary business is the retail sale of goods and services to customers and provides limited financial services such as the issuance of credit cards or in-store financing to customers.

**Food and drink establishment.** The term "food and drink establishment" means an establishment that gives or offers for sale food or beverages to the public for consumption or use on or off the premises, or on or off a pushcart, stand or vehicle.

**Place of entertainment.** The term "place of entertainment" means any privately or publicly owned and operated entertainment facility, such as a theater, stadium, arena, racetrack, museum, amusement park, observatory, or other place where attractions, performances, concerts, exhibits, athletic games or contests are held.

**Retail store.** The term "retail store" means an establishment wherein consumer commodities are sold, displayed or offered for sale, or where services are provided to consumers at retail.

(L.L. 2021/003, 1/10/2021, eff. 7/9/2021)

### § 22-1202 Collection, use, and retention of biometric identifier information.

a. Any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable.

b. It shall be unlawful to sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information.

(L.L. 2021/003, 1/10/2021, eff. 7/9/2021)

### § 22-1203 Private right of action.

A person who is aggrieved by a violation of this chapter may commence an action in a court of competent jurisdiction on his or her own behalf against an offending party. At least 30 days prior to initiating any action against a commercial establishment for a violation of subdivision a of section 22-1202, the aggrieved person shall provide written notice to the commercial establishment setting forth such person's allegation. If, within 30 days, the commercial establishment cures the violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action may be initiated against the commercial establishment for such violation. If a commercial establishment continues to violate subdivision a of section 22-1202, the aggrieved person may initiate an action against such establishment. No prior written notice is required for actions alleging a violation of subdivision b of section 22-1202. A prevailing party may recover:

1. For each violation of subdivision a of section 22-1202, damages of \$500;
2. For each negligent violation of subdivision b of section 22-1202, damages of \$500;
3. For each intentional or reckless violation of subdivision b of section 22-1202, damages of \$5,000;
4. Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
5. Other relief, including an injunction, as the court may deem appropriate.

(L.L. 2021/003, 1/10/2021, eff. 7/9/2021)

### § 22-1204 Applicability.

a. Nothing in this chapter shall apply to the collection, storage, sharing or use of biometric identifier information by government agencies, employees or agents.

b. The disclosure required by subdivision a of section 22-1202 shall not apply to:

1. Financial institutions.

2. Biometric identifier information collected through photographs or video recordings, if: (i) the images or videos collected are not analyzed by software or applications that identify, or that assist with the identification of, individuals based on physiological or biological characteristics, and (ii) the images or video are not shared with, sold or leased to third-parties other than law enforcement agencies.

(L.L. 2021/003, 1/10/2021, eff. 7/9/2021)

### § 22-1205 Outreach and education.

The chief privacy officer shall conduct or facilitate, with any other relevant agency or office, outreach and education efforts, through guidance posted on city websites or through such other means as may be feasible, to inform commercial establishments likely to be affected by this chapter about its requirements.

