THEODORE ROOSEVELT AMERICAN INN OF COURT

Tuesday May 20 6:00 PM

At the offices of
Meyer, Suozzi, English & Klien, P.C.
990 Stewart Avenue
Suite 300
Garden City, NY 11530-4822

Program Title: ***You've Been Hacked. Now What? Cybersecurity and Incident Response for Law Firms Navigating a Data Breach***.

Program Overview: The program will provide Inn Members with a comprehensive overview of their ethical and legal obligations regarding data security and response to a cyberattack. It will cover key legal frameworks such as the New York SHIELD Act and HIPAA, explore relevant New York Rules of Professional Conduct, and offer practical guidance on preventing and responding to data breaches.

Credits: 2.0 CLE credits (1.0 Ethics, 1.0 Cybersecurity Law)

Special Guest and Presenters:

Eric H. Gruber, Esq.
Cooperman Lester Miller Gruber Kraus LLP - Chair

Jessica Lynn Bornes, Esq.
Coffey Modica LLP

Hon. David I. Levine
Judge, Nassau County District Court

Sanford Strenger, Esq.
Salamon, Gruber, Blaymore & Strenger, P.C.

Hon. Ira B. Warshawsky (retired)
Meyer, Suozzi, English & Klien, P.C.

Special Guest - Joseph V. DeMarco, Esq.
DeMarco Law, PLLC

CLM COOPERMAN LESTER MILLER
GRUBER KRAUS LLP

ATTORNEYS-AT-LAW
1129 Northern Boulevard, Suite 402
Manhasset, New York 11030
(516) 365-1400
www.clmlaw.com

Eric H. Gruber, Esq.
Direct Dial: (516) 858-3480
egruber@clmlaw.com

New York City Office
767 Third Avenue
New York, NY 10017
(212) 688-7000

Mr. Gruber is a co-managing partner of Cooperman Lester Miller Gruber Kraus LLP and heads the firm’s Litigation Department. Over almost 40 years, Mr. Gruber has developed a diversified commercial and corporate practice representing domestic and international public and privately-owned companies, entrepreneurs, family businesses and individuals over a range of practice areas including litigation, dispute resolution business transactions and corporate matters.

Mr. Gruber is an experienced litigator in all types of commercial and business issues and an accomplished trial attorney regularly practicing in state and federal courts, as well as in alternative dispute proceedings. Keenly aware of the stresses that litigation can cause a client, Mr. Gruber works with his clients to craft legal strategies for a broad range of civil cases and arbitrations and achieve results that others considered unachievable.

Mr. Gruber has represented plaintiffs and defendants in various matters across a spectrum of substantive areas, including commercial and contract disputes, business torts, corporate and partnership disputes, real estate, construction, creditors’ rights including bankruptcy, and general business law in the federal and state trial and appellate courts and before various arbitration and mediation panels and bodies.

On the transactional side, Mr. Gruber has experience in asset-based lending and other areas of commercial finance, including bankruptcy matters, workouts and turn-around situations. He has actively represented clients in the documentation of commercial finance and equipment leasing transactions and negotiated and papered restructurings on behalf of and with lenders and servicers.

Mr. Gruber often serves as outside general counsel to his clients. In that capacity Mr. Gruber’s clients regularly seek his guidance and counsel on mergers, acquisitions, sales, board advisory and corporate governance issues, risk management, business succession planning, joint ventures, executive compensation, strategic relationships, licensing, business restructuring and recovery, and almost every aspect of the client’s business.

Mr. Gruber has guest lectured on litigation practice at Touro Law School and has lectured for various professional groups and organizations including the Nassau Academy of Law on points of legal procedure and litigation including provisional remedies, discovery, trial practice, business divorces, dissolutions of businesses, disputes between shareholders, and real estate issues.

Mr. Gruber is admitted in the United States Court of Appeals for the Second Circuit, the United States District Court for the Southern and Eastern Districts of New York, and in all of the Courts of the State of New York.

Mr. Gruber is an Executive Committee Member of the prestigious Theodore Roosevelt American Inn of Court, a Past President of B’nai B’rith’s Banking and Finance Unit, and a member of the New York State and Nassau County Bar Associations.

Education

Syracuse University College of Law,
J.D., 1986

Honors
Syracuse Law Review Editor;
Exceptional Editor’s Award

State University of New York at Albany,
B.A. 1983

Jessica Bornes
Associate
Coffey Modica LLP
1377 Motor Parkway, Suite 212
Islandia, New York 11749
914-221-6509 office
516-710-9136 mobile
jbornes@coffeymodica.com

Jessica is an associate at Coffey Modica LLP, where she represents individuals and businesses from the initial service of a complaint through resolution. Her assertive approach, which aims toward a defense-friendly narrative, favorably positions cases for summary judgment and trial.

Jessica obtained her JD from the George Mason University School of Law, where she served on the George Mason Law Review, Trial Advocacy Association, and Moot Court Board. She obtained her BS in Business Administration**,** with a concentration in marketing and a minor in political science, from the University at Buffalo, where she participated in the National Society of Collegiate Scholars and Beta Gamma Sigma Business Honors Society and graduated with distinction.

Jessica is licensed to practice law in New York, New Jersey and Virginia.

Judge David I. Levine
Nassau District Court

Judge David Levine was appointed to the District Court in April 2021 and was subsequently elected to a six-year term. He currently presides over criminal matters.

Prior to his election, Judge Levine maintained a private practice specializing in criminal defense and guardianship manners. From 1990 through 1997, he was an Assistant District Attorney in Queens County, NY. Over the course of his pre-judicial legal career, he litigated over 100 jury trials and countless non-jury proceedings.

Judge Levine was a member of the Board of Zoning and Appeals for the Town of North Hempstead from 2012 through 2021. He had previously been a member of the Town's Ecological Commission.

Judge Levine received a JD from New York Law School and a BA from Binghamton University where he was a founding father of the Sigma Alpha Epsilon (SAE) fraternity chapter.

Judge Levine's involvement in the legal community includes being Past President of both the Queens County Assistant District Attorney's Association and the Criminal Courts Bar Association of Nassau County. He currently serves on the Nassau Academy of Law advisory committee. He is a member of numerous professional organizations.

He is admitted in New York (1990), the local Federal Courts (1993), and the United States Supreme Court (2013).

Judge Levine currently sits on the Long Island Regional Board of the Jewish National Fund (JNF) as well as the Regional Board of Federation of Jewish Men's Clubs (FJMC). He and his wife are active in many local and national charities.

STRENGER BIO.

SANFORD STRENGER, ESQ.

SALAMON, GRUBER, BLAYMORE & STRENGER, P.C.
SUITE 102
97 POWERHOUSE ROAD
ROSLYN HEIGHTS, NEW YORK 11577
516-625-1700 ext. 130

Mr. Strenger, a partner of the firm, has represented businesses and individuals in federal and state trial and appellate courts, administrative agencies, arbitrations and in transactional matters. He has tried matters involving commercial disputes, including corporate, partnership and shareholder disputes, UCC and general contract actions as well as real property actions. In addition, Mr. Strenger has represented clients in the health care industry with emphasis on nursing home corporate governance and transactional matters. He has also represented clients in technology disputes and has counseled clients on the formation of startup technology companies.

Mr. Strenger was an initial member of the NYS Bar Association's Committee on Technology and the Legal Profession and has lectured on cyber security issues and taught electronic evidence in court proceedings at several area Law Schools.

He is the Immediate Past President of the Nassau County Bar Association and a member of NYS Bar Association's House of Delegates.

Mr. Strenger is admitted to practice law in the States of New York and New Jersey and in Federal Court in the Eastern and Southern Districts of New York, the District of New Jersey and Second Circuit Court of Appeals.

A graduate of the Bronx High School of Science at a time when it was the only High School in the United States that had a computer main frame (well before the invention of the personal computer) and taught its students computer languages which today are considered ancient languages. Mr. Strenger availed himself at that time of this ancient learning.

He is a graduate of the University of Rochester, undergraduate, and received a Master’s of Science in Public Policy Analysis from that institution. While in Graduate School Mr. Strenger interned at the United States Congress Office of Technology Assessment and was a contributor to its report to Congress on Managing Commercial High-Level Radioactive Waste.

E-MAIL sstrenger@sgnblaw.com

Justice Ira B. Warshawsky (ret)

Justice Warshawsky started his career in public service as a Legal Aid attorney in 1970 when he was Assistant Chief of the Family Court branch in Queens County. He served as a Nassau County Assistant District Attorney in the District and County Court trial bureaus from 1972 to 1974. Following these four years of prosecution and defense work he became a law secretary, serving judges of the New York State Court of Claims and County Court of Nassau County. In 1987 he was elected to the District Court and served there until 1997. He was elected in 1997 to the Supreme Court of the State of New York where he presided in a Dedicated Matrimonial Part, a Differentiated Case Management Part and sat in one of the county's three Dedicated Commercial Parts. The judge retired at the end of 2011.

In 2012 he joined the law firm of Meyer, Suozzi English & Klein, PC and is Of Counsel in the firm's Garden City, NY office in their Litigation & Alternative Dispute Resolution sections, serving not only as an advocate but as a mediator, arbitrator, litigator, private judge and referee, especially in the area of business disputes and the resolution of electronic discovery(E-Discovery) issues. The judge also serves as a Arbitrator and Mediator for NAM (National Arbitration and Mediation) as well as for the Nassau County Bar Association's ADR Panels and is the current Chair of its ADR Advisory Council.

The Judge received his undergraduate education at Rutgers University (B.A., 1966) and his J.D. degree from Brooklyn Law School (1969).

He has been active in numerous legal, educational and charitable organizations during his career. He is a former director of the Nassau County Bar Association, has served as chair of its Community Relations and Public Education Committee and is a former dean of the Nassau Academy of Law. He is a past president of the Nassau County District Court Judge's Association and the Former Assistant District Attorneys Association of Nassau County. Judge Warshawsky is also a member of the American Bar Association, the New York State Bar Association, the Jewish Lawyers Association and the Theodore Roosevelt American Inn of Court of which he is a past president. He is also past President of the American College of Business Court Judges, of which he is a founding member. He currently serves as a member of the Judicial Advisory Board of the Sedona Conference.

The Judge has served as a lecturer in various areas of commercial, criminal and civil law. He frequently lectures for the National Institute of Trial Advocacy (NITA) at Hofstra and Widener Law Schools. He has lectured for the American, New York State and Nassau bar associations, and private corporate forums, most recently in the area of electronic discovery and Cyber Security. The Judge currently serves as a contributing editor of the Benchbook for Trial Judges published by the Supreme Court Justices Association of the State of New York.

In 1996 the Judge was the recipient of EAC's (Education Assistance Corporation) Humanitarian of the Year Award, in 1997 he received the Nassau County Bar Association President's Award, in 2000 he received the Former Assistant District Attorneys Association's Frank A. Gulotta Criminal Justice Award and in 2004 he received the Nassau Bar Association's Director's Award. Most recently, 2013, he was the recipient of the Jewish Lawyers Association of Nassau County's Paul J. Widlitz Award for service to the Judiciary and the Jewish Community of Nassau County.

He is a past president of the East Meadow Jewish Community Relation Council.

The Judge is past president of the Community Reform Temple of Westbury, Long Island and Vice-president Temple Or-Elohim, ACRC of Jericho, on Long Islandof its Men's Club.

He has been active on the national scene with the Men of Reform Judaism and its predecessor, the North American Federation Of Temple Brotherhoods for over 30 years and is a Past President of the Men of Reform Judaism. The Judge has also served as a Vice President of the NY region of the URJ (Union for Reform Judaism) sitting nationally on the Commision for Social Action, the Committee of Family Concerns and the Youth Committee.

The Judge was married to his wife, Flory, for nearly 52 years. She passed away in 2020. They have two sons, Jason, a bioelectrical engineer living in Newberg, Oregon and Bryan, a teacher, living in Boulder Creek, CA.

BIOGRAPHY

Joseph V. DeMarco
Partner

DeMarco Law, PLLC
99 Park Avenue, Suite 1100
New York, New York 10016
M: 917-576-2369
T: 212.922.9499
F: 212.922.1799
jvd@demarcolaw.com
www.demarcolaw.com

Joseph V. DeMarco is a founding partner of DeMarco Law, PLLC, where he specializes in litigation and counseling in complex matters involving artificial intelligence (AI) law and policy, crypto-currency crimes and frauds, identity theft, hacking and other forms of computer intrusions, surreptitious surveillance, data privacy and security, and the lawful use of new technology. His years of experience in private practice and government handling the most difficult cybercrime investigations and disputes have made him one of the nation's leading lawyers on cybercrime, identity theft, and the law of data privacy and security. He has experience in both civil and criminal litigation and developing compliance policies and programs designed to avoid litigation

From 1997 to 2007, Mr. DeMarco served an Assistant United States Attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property Program (CHIPs), a group of prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws and intellectual property offenses. Under his leadership, cybercrime prosecutions grew from a trickle in 1997 to a top priority of the United States Attorney's Office, encompassing all forms of criminal activity affecting e-commerce and critical infrastructures including computer hacking crimes; large scale on-line frauds and identity theft schemes; and crypto-currency and fintech-related frauds. As a recognized expert in the field, Mr. DeMarco was also frequently asked to counsel prosecutors and law enforcement agents regarding novel investigative and surveillance techniques and electronic evidence collection methodologies. In 2001, Mr. DeMarco served as a visiting Trial Attorney at the Department of Justice Computer Crimes and Intellectual Property Section in Washington, D.C.

Since founding his Firm in 2007, Mr. DeMarco has represented corporations and organizations in various industries in litigation, investigation and counseling matters concerning AI, machine learning, hacking, financial crimes and frauds, theft, and embezzlement facilitated through the use of computers and the Internet. His clients come from a range of industries including media and entertainment (including new media) finance, technology, banking, transportation and logistics, and online and brick-and-mortar retail.

In addition to his counsel practice, Mr. DeMarco has an active practice as an independent arbitrator and monitor. He is on the National Roster of approved neutrals of the American Arbitration Association (AAA) and of Federal Arbitration, Inc. (FedArb), and has significant experience as an Arbitrator including experience adjudicating disputes between businesses involving disputes involving computer hacking, data privacy and security, illegal content monitoring and related business torts. He has also served as a Court-appointed receiver in a contested federal criminal case turning on disputed computer evidence and has also served as an integrity monitor in criminal matters involving high-technology issues and digital evidence.

Since 2002, Mr. DeMarco has served as an adjunct professor at Columbia Law School, where he teaches the upper-class *Internet and Computer Crimes* seminar focusing on, among other things, federal criminal investigations and the novel challenges posed by electronic search and seizure issues. He has spoken throughout the world on electronic evidence preservation and collection in criminal cases, digital investigations, cybercrime, e-Commerce, and IP enforcement, including at the Practicing Law Institute (PLI), the National Advocacy Center, and the FBI Academy in Quantico, Virginia. He has also served as an instructor on cybercrime law to judges at the New York State Judicial Institute.

Prior to joining the United States Attorney's Office, Mr. DeMarco was a litigation associate at Cravath, Swaine & Moore, where he concentrated on intellectual property, antitrust, and securities litigation. Between law school and Cravath, Mr. DeMarco served as a Law Clerk to the Honorable J. Daniel Mahoney of the United States Court of Appeals for the Second Circuit.

Mr. DeMarco holds a J.D. *cum laude* from New York University School of Law where he was an Articles Editor of the *NYU Law Review* and a member of the Order of the Coif. He received his B.S.F.S. *summa cum laude* from the School of Foreign Service at Georgetown University. He is currently a member of several bar and professional associations, including the:

- International Bar Association (Technology Committee)
- International Association of Korean Lawyers (Past Member, Board of Directors)
- Federal Bar Council
- New York State Bar Association, Commercial and Federal Litigation Section (Past Co-chair, Internet and IP Committee) and Dispute Resolution Section
- New York City Bar Association (past Chair, Information Technology Committee)

Mr. DeMarco is a *Martindale-Hubbell* AV-rated lawyer for Computers and Software, Litigation and Internet Law, and is listed in *Chambers USA: America's Leading Lawyers for Business* in Privacy and Data Security law. He has been named as a "*SuperLawyer"* in Intellectual Property Litigation. He is a member of the Professional Editorial Board of the *Computer Law & Security Review* and serves on the Board of Advisors of the *Center for Law and Information Policy* at Fordham University School of Law. He was recently appointed by the Connecticut General Assembly to advise that body on data privacy law issues including those impacted by Connecticut's recently enacted data privacy law.

Mr. DeMarco has received numerous professional awards, including the U.S. Department of Justice *Director's Award for Superior Performance* and the *Lawyer of Integrity Award* from the Institute for Jewish Humanities.

Outline
May 20 Cyber Security Inns of Court Program

Program Title:

***<u>You've Been Hacked. Now What? Cybersecurity and Incident Response for Law Firms Navigating a Data Breach</u>*.**

Program Overview:

- The program aims to provide Inn Members with a comprehensive overview of their ethical and legal obligations regarding data security. It will cover key legal frameworks such as the New York SHIELD Act and HIPAA, explore relevant New York Rules of Professional Conduct, and offer practical guidance on preventing and responding to data breaches. We will use case studies, skits, and interactive discussions intended to provide attendees with insights to protect client data and ensure compliance.
- **Credits:** 2.0 CLE credits (1.0 Ethics, 1.0 Cybersecurity Law)

I. Introduction & Course Overview

- **Why This Matters:** Provide a brief overview of rising cyber threats to law firms. (E.g., roughly *one-quarter* of law firms have experienced a security breach, and phishing is a leading cause.) Emphasize that *all* practice areas handle sensitive data vulnerable to breaches. Lawyers have professional and legal obligations to safeguard client information – a breach can harm clients and lead to liability or ethical violations.
- **Learning Objectives:** By the end, participants should be able to: 1) Identify key compliance duties under the New York SHIELD Act and HIPAA in a breach scenario; 2) Understand ethical duties under NY Rules 1.1, 1.4, 1.6, 5.1, 5.2, 5.3 in the context of cybersecurity; 3) Implement an incident response plan and best practices for breach notification; 4) Integrate cybersecurity risk management into their daily practice to prevent violations.

II. Legal and Ethical Framework Overview (20 minutes)

- **New York SHIELD Act – Compliance Essentials:**
    1. Outline NY's Stop Hacks and Improve Electronic Data Security Act. It imposes a duty on businesses (including law firms) to implement "**reasonable administrative, technical, and physical safeguards**" for private information (PI).

2. Discuss examples of required measures (security program coordinator, risk assessments, employee training, secure service providers, etc.) and note that lacking these could invite enforcement.
3. Failure to comply with the SHIELD Act can result in significant penalties:
   - Up to $250,000 for delayed breach notifications.
   - Up to $5,000 per violation for failing to implement safeguards.
   - The New York Attorney General may also seek restitution or injunctive relief.
4. Review SHIELD Act breach notification rules: notify affected individuals and the NY Attorney General (using AG's online portal) in the "most expedient time possible" after discovery.
5. If over 5,000 NY residents are affected, consumer reporting agencies must be notified.

- **HIPAA Breach Obligations:**
  1. If the firm handles protected health information (PHI) as a business associate of healthcare clients, HIPAA's rules apply.
  2. **When HIPAA Applies:**
     - Law firms can be **Business Associates** under HIPAA when they handle Protected Health Information (PHI) on behalf of healthcare clients (e.g. in malpractice, personal injury, workers' comp, etc.).
     - Define PHI (individually identifiable health information in any form) examples relevant to lawyers (medical records, patient lists in client files).
  3. **Business Associate Agreements (BAAs):**
     - Covered entities (health providers, plans, etc.) are required to have BAAs with law firms (their BAs).
     - The BAA contractually obligates the firm to safeguard PHI and report breaches.

        - If practice involves client health data, they should have signed a BAA – a reminder of their direct compliance duties.

    4. **Breach Notification Rule:** What happens if a law firm (BA) has a breach involving PHI:

        - The firm **must notify the covered entity without unreasonable delay and no later than 60 days after discovering the breach**. (The 60-day requirement is addressed in the skit.)

        - The notice to the covered entity should include information for the covered entity to fulfill its obligations (so the hospital/client can notify affected patients, HHS, and if >500 people, the media).

        - If the law firm is itself a covered entity (rare, but e.g. if managing a self-insured health plan for employees), it would directly notify individuals and HHS.

    5. **HIPAA Security/Privacy Standards:**

        - Highlight that beyond breach notification, HIPAA imposes ongoing duties to protect electronic PHI (administrative security policies, access controls, etc.).

        - This dovetails with what “reasonable efforts” under Rule 1.6 and “reasonable safeguards” under SHIELD mean in practice – e.g. encryption, training staff, etc.

    6. **Consequences:** Note potential penalties for HIPAA violations (OCR enforcement, hefty fines) to convey the risk.

- **Ethical Duties of Lawyers (NY Rules):** Attorneys must consider not just laws like SHIELD/HIPAA, but also their ethical obligations during cybersecurity incidents. Introduce the key NY Rules of Professional Conduct that will be woven into the case:

    1. **Rule 1.1 – Competence:**

        - Lawyers must provide competent representation, which *now includes technological competence*. Commentators (and NY ethics opinions) emphasize that lawyers should understand the basics of cybersecurity and use reasonable security measures to protect client data. Failing to keep up with tech or to prepare for cyber risks (e.g., not having any incident response plan) can be a lapse in competence.

- NY, like many states, expects attorneys to understand the basics of the technology they use and the cybersecurity risks involved. An attorney doesn't have to be an IT expert, but must either develop competence or consult tech professionals.

2. **Rule 1.4 – Communication:**

    - Lawyers have a duty to keep clients reasonably informed and to explain matters so clients can make informed decisions. A data breach affecting client information is unquestionably a **"material development"** in a matter that **must be communicated to the client promptly**.

    - Ethical guidance (including ABA Formal Opinion 483) considers client notification obligatory when their confidential data is compromised.

    - Outline what a proper client notice looks like ethically: it should be prompt and include sufficient detail (nature of breach, data affected, remedial steps, and guidance to client)

3. **Rule 1.6 – Confidentiality:**

    - Attorneys have a duty to protect client confidences. New York's Rule 1.6(c) affirmatively requires lawyers to make reasonable efforts to prevent unauthorized access or disclosure of client information. This creates an ethical mandate to implement cybersecurity safeguards. Connect this to the SHIELD Act's safeguard requirement (reasonable security): both law and ethics demand proactive protection. Discuss factors that determine "reasonable" efforts (sensitivity of information, cost of safeguards, difficulty of implementation, etc.).

    - If a breach occurs, Rule 1.6 also governs what disclosures are permissible: lawyers may need to reveal some info to law enforcement, insurers, or experts to respond to the breach – such disclosures are generally allowed if they are "impliedly authorized" to serve the client's interests or if the client gives informed consent.

4. **Rule 5.1 – Responsibilities of Partners/Managers:**

    - Firm leaders must make reasonable efforts to ensure the firm has measures in place for all lawyers to comply with ethical rules. This means partners should institute appropriate cybersecurity policies, training, and supervision. If a firm's leadership is lax about cyber protections, they could be violating Rule 5.1 by failing to safeguard client data and supervise compliance.

5. **Rule 5.2 – Subordinate Lawyers:**

    - Subordinate attorneys have their own duty to follow the Rules, even if acting at direction of a supervisor. They are protected if they follow a supervisor's reasonable resolution of an arguable question, but cannot just "follow orders" if instructed to act unethically.

    - In a breach context, if a supervising partner decided to conceal a breach or not notify clients, a junior lawyer could not simply go along without running afoul of Rule 1.4 and 1.6. This rule empowers associates to push for ethical handling of cybersecurity issues.

6. **Rule 5.3 – Non-lawyer Assistants:**

    - Lawyers must ensure that non-lawyer staff (e.g. IT managers, paralegals) and outside vendors are properly supervised regarding client data. This includes making sure IT personnel uphold confidentiality and follow security protocols.

    - If a firm uses an outside IT provider or forensic investigator, Rule 5.3 requires due diligence and oversight (e.g., confidentiality agreements, vetting security practices.

- **4,5 AND 6 *TEACHING POINT*:** Tie these to a phishing breach aspect or caused by human error – if the breach resulted from an employee's mistake (as often happens via phishing), did the firm have adequate training and policies?

    - Under 5.1/5.2/5.3, partners could be responsible if they failed to establish reasonable tech guidelines or vet an IT vendor.

        - *"What ongoing steps should the firm's partners take after an incident to uphold their 5.1/5.2/5.3 duties?"* (update security protocols, mandate firm-wide cybersecurity training, s hire outside experts to audit systems, etc.)

- **ABA Formal Opinion 483 (2018) – "Lawyers' Obligations After an Electronic Data Breach or Cyberattack":** Key points:
    - Lawyers must employ reasonable efforts to monitor for breaches (you can't just ignore signs of intrusion).
    - If a breach is detected, **act reasonably and promptly to stop it and mitigate damage.** This is part of competence and safeguarding client property.
    - **Notify clients** of a breach when it's likely their material confidential information was accessed or lost. Not every hack requires client notice (e.g., if no client data was compromised), but if client info is at risk, the client has the right to know. This ties into Rule 1.4's duty to communicate.
    - The opinion strongly suggests having an incident response plan *"in place long before a breach ever occurs"* implying that preparedness is part of ethical competence.
- **Key New York Ethics Opinions:** Note that NY's ethics authorities echo these principles:
    - *NYSBA Opinion 842 (2010)* allowed cloud data storage if lawyers use reasonable care (e.g., encryption, due diligence on provider), and advised lawyers to stay abreast of tech advances to protect confidentiality.
    - *NYSBA Opinion 1019 (2014)* approved remote access to client files from home if the firm uses adequate security or client consent, underscoring "reasonable protection" for confidentiality in any tech use.
    - *NYCLA Opinion 749 (2017)* explicitly addressed cybersecurity and competence, stating that a lawyer's duty of competence extends to having the technological knowledge to secure client data, or consulting

with someone who does. It connects Rules 1.1, 1.6, 5.1, and 5.3 to cybersecurity practices.

- *NYSBA Opinion 1240 (04/08/2022)* If the attorney's smartphone "contacts" folder contains "confidential" client information, the attorney may not consent to share the contacts folder with a smartphone app, unless the attorney determines that (1) no person will view the information and (2) the information will not be sold or transferred to additional third parties, without the client's consent. Emphasizes how seriously NY takes the duty to prevent unauthorized access under Rule 1.6(c).

- *NYC Bar Op. 2024-3* concludes in the event of a cybersecurity incident (1), lawyers have ethical obligations to protect clients' confidential information; (2) there are statutory and regulatory notification requirements and ethical obligations under Rule 1.4 to promptly notify current clients of the compromise of the confidentiality or if the law firm will likely be unable to meet material obligations to the client; (3) there is no ethical prohibition against, or requirement to, pay a ransom to a cyber extortionist, and lawyers and law firms may be not candid with respect to certain material facts when negotiating with cyber-extortionists in efforts to protect or regain access to client information and firm systems; (4) lawyers and law firms can only disclose client confidential information to law enforcement or in connection with a government investigation of a cybersecurity event if permitted by Rules 1.6, 1.9 or 1.18 and should be cognizant of potential risks to their clients of communicating with law enforcement or other government officials; and (5) conflicts of interests may require the lawyer or law firm not to advise a client in connection with the cybersecurity incident or to cease representing the client altogether in the event of a malpractice claim arising from the incident

III. Initial Response Priorities:

- Highlight best practices immediately post-breach:

- *Containment:* The firm isolated affected systems, changed passwords. This aligns with the duty to mitigate harm promptly (as Formal Op. 483 advises).

- *Investigation:* It's mentioned they are still investigating what data was viewed or taken. Stress the need to preserve evidence (IT should save log files, etc., which the skit will show later for forensic analysis and possibly law enforcement.

- *Notification (Internal):* The Managing Partner immediately looped in key people – this shows good leadership (Rule 5.1) by assembling a team (legal and technical) to handle the incident. They involve Outside Breach Counsel (for legal compliance guidance) and Insurance Counsel (to navigate cyber insurance).
- *Ethical Reflections:* Even at this early stage, ethical duties are present. The Managing Partner shows awareness: "We must handle this by the book – both law and ethics. This is exactly the mindset Rule 1.1 competence demands in a crisis.
    - Mention that if a firm had **no clue what to do** (no written incident response plan, no expert to call), that could be a failure of competence. Here, bringing in outside experts is a smart way to fulfill competence if the firm lacks in-house knowledge (lawyers can associate with those who have the requisite tech expertise).
    - Also note: Rule 5.3 duty to supervise non-lawyers means the firm should empower the IT Manager with clear policies on breach handling. It seems IT did the right thing by immediately reporting up the chain – an ethic of openness that firm leadership should foster.

IV. "Emergency Strategy Meeting"

Legal Compliance Topics:

- discuss the legal duties being addressed:
- **Breach Notification Law (SHIELD Act):** Outside Counsel explains they must notify affected individuals whose "private information" was exposed, under New York law.
- Discuss what *counts* as "private information" in NY (e.g., combination of name with SSN, driver's license, account numbers, biometric data, usernames with passwords, etc., and also certain health info).
- In the scenario, client data included financial records and possibly litigation data with personal info, so NY notification likely applies.

- **Notify the NY Attorney General:**
  - The firm will report via the AG's breach portal, which will also notify state police and state consumer protection.
  - Managing Partner agrees that they'll be notifying law enforcement as appropriate.
  - Emphasize that under the SHIELD Act, if *over 500 NY residents* are impacted, they must also notify the state Attorney General's office within 10 days of determination (even if individual notice isn't required due to certain exceptions).
- **Timing:** "Most expedient time possible" – note that a prompt response is required, but after securing the system (containment comes first, as they've done).
- **Content of Notices:** They will need to include in the individual notices a description of the incident and types of data compromised, which Outside Counsel will help draft (we'll revisit this in Scene 3 with the client notification letter).
- **Penalties:**
  - Insurance Counsel warns that if they hadn't had required safeguards, the NY AG could penalize the firm (he mentions "up to $5,000 per failed safeguard" in the skit). This refers to SHIELD Act's penalties for not having reasonable security measures.
  - Also, failing to notify could result in fines ($20 per instance, up to $250k). The team clearly wants to avoid any compliance misstep.

- **HIPAA and Other Laws:**
  - The Outside Counsel asks if any protected health information was breached (IT had mentioned healthcare info was possibly compromised). If yes, and the firm is a business associate, they must also follow HIPAA's breach requirements.

    - In the skit, they specifically mention notifying any of the client's employees or patients if their personal data is involved, implying coordination with the client on those notices.

    - Discuss that the firm would also inform the healthcare client so the client can fulfill any **HIPAA** obligations. (note cross-jurisdiction issues: if data of individuals from other states is involved, those states' breach laws may require notice too. Typically, law firms have to comply with each applicable state law in a multi-state breach.)

- **Cyber Insurance Procedures:**

- Insurance Counsel highlights the firm's **cyber insurance policy** – it can cover many breach response costs (forensics, notification, credit monitoring, legal fees, even ransom payments). But to utilize coverage, the firm must **promptly notify the insurer**.

- In the skit, IC gave preliminary notice that morning.

- Discuss the practical tip: always review your insurance policy's terms *before* an incident. Policies often require notice within a short window and use of insurer-approved vendors for things like forensics or public relations. Failing to follow those can jeopardize coverage.

- **Involving Law Enforcement:**

    - The team contemplates whether to alert law enforcement (e.g., FBI cybercrime, local police). Outside Counsel suggests it's often wise, especially since financial data and identity theft risk are at play.

    - In New York, submitting the breach notice to the AG can trigger law enforcement involvement, but proactively reaching out can show good faith.

    - Stress that involving law enforcement can help in investigation and is encouraged unless there's a specific reason not to (like protecting privileged info – but here it's a third-party hacker, not an internal theft by a client or something). It can also be part of fulfilling ethical duties – showing the firm isn't hiding anything.

- **Ethical Duties & Decisions:**
    - When the IT Manager sheepishly asks if they "did enough to protect the data in the first place," Insurance Counsel notes the SHIELD Act's safeguards requirement and hints at potential **malpractice liability**. *What does technological competence entail?*
        - It means lawyers must understand the basics of the tech they use and the risks involved. If they lack knowledge, they must consult someone with expertise or get training. In practice, a managing partner must ensure the firm uses reasonable security (e.g., up-to-date firewall, encryption, etc.). The skit gives an example: storing sensitive client data unencrypted in the cloud or a server without safeguards could be a lapse in tech competence.
        - Also Rule 1.6's duty to safeguard confidential info.
    - **Rule 5.1 & 5.3 – Firm Management:**
        - Skit identifies Rules 5.1 and 5.3, reminding that firm leadership is accountable for policies and supervision to protect client info.
        - **Discuss:** Was the firm in compliance? Did the partners set appropriate policies? The script implies they had some security measures but perhaps not all (they mention planned improvements like multi-factor authentication had been delayed).
        - **Teaching Point:** partners should not procrastinate on security initiatives. They should conduct regular risk assessments and trainings (explicitly required by SHIELD Act and by ethical duty).
            - If a breach occurs and it's found the firm ignored known security gaps (like not implementing MFA which could have prevented the phishing exploit), that could breach Rule 5.1/5.3 responsibilities, and even hint at negligence.
    - **Rule 1.6 – Confidentiality & Breach Response:**
        - There's an interesting ethical point raised: Insurance Counsel says firms *without* an incident response plan will likely be found to have violated Rule 1.6 if a breach compromises client.

    - Can failing to plan be an ethical issue? Many might not have thought of it that way, but ABA Op. 483 suggests an incident response plan is a matter of professional responsibility. So, tie this to Rule 1.6 and 1.1: reasonable preparedness is part of preventing unauthorized disclosure and competently safeguarding data. Not having a plan can lead to chaotic or delayed responses (i.e., a worse breach outcome, which means not making "reasonable efforts" as 1.6(c) requires).

- **Rule 1.4 – Communication (When to tell clients?):**

    - Decide **when and how to notify clients**. This is a crucial ethical judgment call.

    - *Should the firm notify clients immediately, before knowing all details, or wait until they have a fuller picture?*

    - Likely, a best practice is to notify affected clients promptly but with enough information to be useful – perhaps after initial containment and initial forensic analysis (which is often within days, not months). ABA Formal Op. 483 doesn't specify an exact timeframe, but it implies prompt communication once material info is known.

    - Rule 1.4 in NY says lawyers must keep clients reasonably informed and promptly convey important information.

    - In the skit, they don't notify clients in Scene 1 (immediate stage) because they were still investigating.

    - By Scene 3 the same day, they do it. It's ethical to take a brief time to investigate so you can give clients accurate, substantive information (and not cause panic with incomplete info), **but** undue delay is not acceptable. If the firm waited weeks with no word, that would violate Rule 1.4's requirement to promptly inform about a material .

    - Also consider that under SHIELD Act, notification to individuals must be made "expeditiously." Both law and ethics favor prompt notice. Encourage a best practice: err on the side of sooner, and certainly **before the client hears about it from another source** (or worse, from the news).

    - **Rule 5.2 – Subordinates:**
        - Who is a subordinate lawyer – perhaps the Insurance Counsel could be an associate at the firm, or imagine there's a junior associate assisting the managing partner. If, hypothetically, a senior partner suggested not telling a particular client about the breach, the junior lawyer should recognize that would violate 1.4 and 1.6. Rule 5.2 would not excuse the junior in participating in concealment. This rule empowers even lower-level lawyers to insist on ethical conduct. "What would you do if a partner said 'maybe we don't tell Client X because it might upset them'?" The hoped-for answer is: advise strongly against that, and if it persisted, one might even have to escalate or withdraw – though hopefully not needed if everyone knows the rules.)
- *"Which legal or ethical obligation has the highest priority in the first 24 hours after a breach?"* (Single choice: A) Preserve client confidentiality; B) Comply with breach notification law; C) Protect the firm's reputation; D) Inform current clients).
    - Discuss that several are *simultaneous* priorities, but if forced to choose, **protecting confidentiality** (stopping the breach) comes first (A). Immediately after, complying with the law (B) and informing clients (D) are critical – in fact, B and D usually align, since the law requires informing clients and authorities, and ethics requires informing clients. "Protect the firm's reputation" (C) is the lowest priority – ethical practice and compliance will in the long run protect reputation better than a cover-up. The poll is a springboard to reiterate: **containment, legal compliance, and client communication** are the core pillars of incident response.
- **Incident Response Checklist In Course Handout:**
    - **Model Incident Response Checklist** provided in the course materials. Walk through how the checklist maps onto what the firm in the case is doing:

2. **Detect and Verify incident** – (Yes, IT noticed unusual activity and confirmed the breach).

3. **Contain** – (Yes, took systems offline, changed passwords).

4. **Assemble Response Team** – (Yes, MP called lawyers, IT, insurance – a multidisciplinary team).

5. **Notify Internal Stakeholders** (firm management, etc.) – (Happening now in the meeting).

6. **Engage Experts (Forensics, Outside Counsel)** – (Yes, outside counsel is on call, forensics likely next step via insurance).

7. **Assess Legal Obligations** – (They are doing that: SHIELD, HIPAA, etc., figuring out who must be notified and by when).

8. **Develop Communication Plan** – (They are planning client notices and possibly public/regulator notices).

9. **Notify Externally** (Clients, AG, law enforcement, insurer) – (In progress; insurer done, next clients and AG).

10. **Document Everything** – (IT Manager will preserve; they'll generate a report later).

11. **Follow-up Remediation** – (They've already started discussing improvements to prevent reoccurrence).

V. "Client Notification and Aftermath" (Scene 3)

- **Ethics of Client Communication:**
    - Analyze call with client in light of Rule 1.4 and Formal Op. 483:
        - The Managing Partner proactively called the client as soon as practicable – this fulfills the duty to **inform the client promptly of the breach**. Ethics opinions stress that hiding a breach is not an option.
        - By being forthright, the firm is complying with Rule 1.4 and ABA 483's guidance that clients must be notified because it impacts their representation.
    - They conveyed facts and next steps clearly, which is crucial for effective communication. The MP did not hide the severity; he apologized and took responsibility. This honesty likely preserved the relationship.

  - Discuss with the audience: *How would you approach such a call?* (Key: express regret, explain what happened, and focus on solutions and protecting the client's interests, as was done here.)

  - Note how the firm also addressed the client's concern about privileged info – an ethical duty (to preserve privilege and confidentiality) extends to after a breach. The firm reassured that privilege is maintained and they would act to protect it if needed.

  -

    - What if the client had asked for even more information, like "Who exactly messed up?" or "How do I know you truly fixed it?" How to balance transparency with not disclosing unnecessary internal details. Generally, you should not scapegoat an employee; it's a firm responsibility. And you might not have all answers immediately (forensic analysis might take days), so it's fine to say investigation is ongoing and they will get a detailed written report soon (which the MP promised).

- **Legal Follow-Through (Breach Notices):**

  - After the call, the firm will send out the **written notifications**. Go over what a good **Breach Notification Letter** contains (see e.g., https://dos.ny.gov/data-security-breach-notification-sample-letter):

  - A description of the incident (in general terms, without revealing sensitive security info that could aid attackers).

  - Types of personal information that were involved (e.g., names, SSNs, financial account numbers, health info, etc.).

  - What the firm is doing about it (e.g., steps taken to secure systems, working with law enforcement, improvements made).

  - What the recipient can do (e.g., advice to monitor accounts, reset passwords, etc., depending on data type).

  - Offer of credit monitoring or identity theft protection if appropriate (in the scenario, the firm's insurance will cover credit monitoring for those affected).

  - Contact information for questions (and possibly information about how to get the free credit monitoring).

  - Any legal notice language required by statute (for example, NY requires including contact info for credit reporting agencies if certain data types were breached).
  - The tone should be empathetic and reassuring, without admitting legal liability outright. It's a fine line: comply with legal notice requirements and be ethical (no misrepresentation), but also these letters often carefully word things under counsel's advice.
- **Regulatory and Other Notifications:**
  - Remind that beyond client and affected individuals, by now the firm also has or will notify:
  - **NY Attorney General** (via the portal, as discussed).
  - **Law enforcement** (they decided to notify FBI/State Police in parallel).
  - **Insurance Carrier** (already done early on).
  - Possibly **professional liability carrier** if there is potential malpractice claim (not explicitly in skit, but a real consideration).
  - If **clients in other jurisdictions** were affected, comply with those jurisdictions' breach laws (mention briefly to close the loop on legal compliance).
  - **Former Clients:** An interesting ethical question raised in the skit – Outside Counsel advises notifying even former clients whose data was in the breached.
    - NY law requires notice to any affected "person" (which could include former clients as their data is personal info). Ethically, Rule 1.9 (duties to former clients) isn't explicitly in the outline, but best practice is to inform them as well.
    - The Managing Partner agrees because it's "the right thing to do".
    - *"If old client files were compromised, are we obligated to notify those former clients?"* Most will likely say it's wise to do so. This shows commitment to confidentiality beyond the end of representation and can prevent later backlash if a former client discovers a breach was hidden from them.

- **Liability and Risk Management:**
    - The client in the scenario hinted at the firm's "negligence" and DCH covering costs. Use this as a springboard to discuss:
    - **Legal Liability:**
        - A law firm could face a malpractice claim if a client is harmed by a breach (e.g., financial loss, case disruption) and the firm failed to meet a standard of care in protecting data. While no private right of action under SHIELD Act, clients can sue under tort or contract theories. The best defenses are demonstrable reasonable security practices and prompt, responsible actions after the breach. The case study firm is doing the right things to mitigate liability: they notified promptly, they're providing credit monitoring (goodwill), and they're improving security.
    - **Ethics Complaints:**
        - Could a client also file a complaint with the disciplinary committee? Possibly, if they felt the firm egregiously mishandled confidential information or kept them in the dark.
        - Mention that there haven't been many reported disciplinary cases for data breaches yet, but theoretically a violation of 1.6 or 1.4 could be grounds for discipline. Again, the firm's transparency and corrective action would likely satisfy regulators that they took the breach seriously (and indeed, Formal Op. 483 would view their actions positively).
    - **Reputation Management:**
        - How a firm handles a breach can become public. If clients are satisfied with the response, they may stick with the firm (as our Client seems likely to, given the reassurances). If a firm tried to hide it and it leaked, the reputational damage could be far worse than the breach itself. This ties into the ethical duty of candor and maintaining the profession's integrity.

VI. Preventative Measures and Lessons Learned

- **Post-Incident Remediation:** In the skit's epilogue, the firm team discusses how they will *"implement that incident response plan we clearly needed"* and bolster security going forward. What are the **preventative steps** every firm should take *now*, before a breach occurs (or to prevent a repeat):
    - **Incident Response Plan:** If attendees remember one thing, it should be to either create or update an incident response plan *immediately*. As Formal Op. 483 and our case study showed, having a plan is critical. The plan should designate roles (who contacts clients, who handles IT tasks, who speaks to media), contact lists (key people, law enforcement, forensic firms), and checklists of steps (like the one we provided) to ensure nothing is overlooked in the heat of the moment.
    - Encourage firms to conduct a *practice drill* or tabletop exercise annually (even something as simple as walking through this case study and asking "what would we do?"). This helps fulfill both the SHIELD Act's training mandate and ethical duty of competence.
    - **Strengthening Safeguards:** The **"reasonable safeguards"** required by law and practical measures:
        - *Technical:*
            - Use strong encryption for sensitive data (in storage and in transit). Implement multi-factor authentication for remote access (no more "password-only" protection). Keep software updated and patched. Utilize intrusion detection systems and regular network monitoring to catch suspicious activity (if possible, 24/7 monitoring or at least daily log reviews). Regularly backup data offline to prepare for ransomware.
        - *Administrative:*
            - Conduct regular cybersecurity training for all employees (phishing simulations, security awareness). Note that the cause of the breach was a phishing email, which training might have prevented.
            - Enforce policies (e.g., acceptable use of devices, strong password policies, mobile device security). Limit access

        permissions on a need-to-know basis (so a single hacked account can't access everything).

        - Vet third-party vendors: ensure cloud providers or IT consultants contractually commit to security standards (this also ties into Rule 5.3 obligations).

    - *Physical:*

        - Secure offices and servers – e.g., keep server rooms locked, use clean-desk policies for sensitive paperwork, dispose of files properly (shredding or secure deletion).

    - These measures not only fulfill legal duties but also ethical **"reasonable efforts"** to prevent disclosure under Rule 1.6. What is "reasonable" evolves – today, encryption and MFA are often considered standard care.

- **Cyber Insurance & Risk Management:**

    - Encourage cyber insurance coverage *before* a breach. As seen, it was very helpful that DCH had insurance and an insurance counsel who knew the ropes.

    - Make sure any firm's policy covers the types of incidents relevant and that key staff know how to activate it. Also, consider client requirements: some clients (especially corporate or healthcare) now expect their law firms to have robust security and may even ask about it in engagements. Being proactive on cybersecurity is becoming part of competent business development.

- **Ethical Culture and Training:**

    - Beyond IT fixes, foster a culture where lawyers and staff take security seriously as part of their ethical duty. Senior partners (Rule 5.1) should lead by example – e.g., actually using secure practices and not trying to bypass them. Subordinate lawyers (Rule 5.2) and staff should feel empowered to report potential security issues or mistakes immediately without fear. The firm in the skit "learned its lesson" and the Managing Partner commits to firm-wide review of policies and training. New York's CLE requirement for cybersecurity means every attorney will at least get periodic training. Firms should leverage that by having attorneys share tips from CLEs or bring in experts for lunch-and-learns.

- **Lessons Learned Recap:**
- Key takeaways from *Dewey Cheatum & Howe's* story:
    - *Preparation is key* – don't wait for a breach to figure out your plan (they wished they had prepared in advance).
    - *Act fast and smart* – contain the damage, involve the right experts, and comply with notification laws.
    - *Communicate openly* – both inside the response team and externally to clients and authorities. Transparency upholds your ethics and preserves trust.
    - *Learn and Improve* – after an incident, do a post-mortem. The skit team plans to write a full incident report and improve their safeguards. Every breach (or even near-miss) is an opportunity to strengthen your practice.
    - *Ethics and Law go hand-in-hand* – by doing the right thing for clients (ethically), the firm also complied with legal duties. This alignment is illustrated by the Managing Partner's closing remark that they complied with SHIELD Act and HIPAA, **"upheld our ethical duties,"** and set a path to stronger security.

VII. Conclusion Program Wrap-Up:

- The case study illustrated the intersection of **cybersecurity compliance** and **legal ethics**. Dewey Cheatum & Howe's experience showed that a law firm can survive a cyber-attack by responding diligently and ethically – and that preparation and honesty are the best policies. They take their obligations under the NY SHIELD Act, HIPAA, and the Rules of Professional Conduct seriously, and are committed to full compliance and ethical practice to protect their clients and the integrity of the profession.

- **Final Takeaway:** Encourage attendees to **take action** at their own organizations – whether it's scheduling a meeting with their IT department to review security, updating client engagement letters to address cybersecurity responsibilities, or simply sharing these insights with colleagues. Stress that *cybersecurity is an ongoing duty* akin to competence and that ethical lawyering in the digital age requires vigilance and continual improvement.

May 20 Cyber Security Inns of Court Program

Program Title:

You've Been Hacked. Now What? Cybersecurity and Incident Response for Law Firms Navigating a Data Breach.

Program Overview:

This evening's program aims to provide you with a comprehensive overview of your ethical and legal obligations regarding data security and following a data breach. Our program is a skit titled "**The Data Breach at Dewey Cheatum & Howe."** It will cover key legal frameworks such as the New York SHIELD Act and HIPAA, explore relevant New York Rules of Professional Conduct, and offer practical guidance on preventing and responding to data breaches.

Characters

- **Managing Partner (MP)** – played by Judge Ira Warshawsky - The head of a small/mid-size NY law firm. Wants to do the right thing legally and ethically but is stressed (and occasionally sarcastic) under pressure.
- **IT Manager (IT)** – played by Sanford "Sandy" Strenger – Is the firm's tech specialist. He is knowledgeable about systems, a bit nervous, and feels responsible.
- **Outside Counsel (OC)** – played by Eric Gruber – Is a cybersecurity attorney brought in to advise on breach response. Expert on laws like the SHIELD Act and HIPAA, with a practical demeanor.
- **Insurance Counsel (IC)** – played by Jessica Bornes – Is the firm's cyber insurance attorney. Focused on complying with insurance requirements and minimizing financial impact, but also contributes to the legal strategy.
- **Client** – played by Judge David Levine - Is a major corporate client of the firm whose sensitive data was compromised. Concerned and upset, demands answers and accountability.

- **Chat JD** – is played by a special guest Joseph DeMarco - A humorous but knowledgeable AI legal assistant (accessed via a smart speaker or laptop). Chat JD provides clear explanations of legal and ethical obligations in a friendly tone. It occasionally cracks light jokes while delivering accurate information.
- I will also be function as this evening's **Facilitator (Moderator)** – I will step in during breaks between scenes to engage with questions or prompts for discussion.

Scene 1: The Breach is Discovered

Setting: Early Monday morning at the law firm **Dewey Cheatum & Howe, LLP**. The Managing Partner walks into the office to find the IT Manager anxiously typing on a laptop.

IT Manager: (frantically typing) Managing Partner, we have a situation. It looks like our network was breached over the weekend. I'm seeing evidence that hackers accessed confidential files – there are signs of large data transfers leaving our system. Hackers accessed confidential files – I'm seeing evidence of data exfiltration.

Managing Partner: Wait, what is data exfiltration**?!**

IT Manager: In layman's terms, data exfiltration is someone secretly sneaking important or private information out of a secure place without permission. Imagine someone quietly copying confidential documents, financial records, or personal files from a business's computers and then sending or taking them elsewhere—usually for malicious reasons or financial gain**. A data breach.**

Managing Partner: (alarmed) A breach? As in someone broke in and stole files? We spend all sorts of money on IT security to prevent this! How could that happen?

IT Manager: (grimacing) Unfortunately, no system is foolproof. Law firms are prime targets for hackers these days — roughly one in four law firms have experienced a security breach. It seems we've just joined that club. From what I can tell, it was a cyber break-in: likely a **phishing** email tricked someone into revealing their password. Once the attackers got in, they accessed our client folders.

Managing Partner: (runs hand through hair) Phishing... I always worry about those scam emails. I wonder which of our folks took the bait. (With dark humor) Hopefully not the associate who fell for that "Earn free CLE credit now!" email last month.

IT Manager: (sheepishly) It can happen to the best of us. Those phishing emails are getting very convincing. All it takes is one careless click.

Managing Partner: (groans) This is bad. Really bad. What types of information did they get? Do we know how much was accessed or taken?

IT Manager: I'm still piecing it together. So far, it appears the attackers accessed a folder with clients' personal information; their names, addresses, Social Security numbers; some financial data including bank account and credit card details related to client billing;

and a batch of medical records we had from a personal injury case. That means potential **personal health information** was compromised. And on top of that, some case files containing confidential attorney-client communications were in the mix. In short: a lot of sensitive stuff.

Managing Partner: (eyes widening) Personal data, financial info, medical records, *and* privileged legal documents… This is a nightmare smorgasbord of a breach.

IT Manager: I know. I've taken steps to **contain the breach** for now — I reset all employee passwords and took the affected servers offline. But we're still investigating exactly what data was viewed or copied – the exfiltration.

Managing Partner: (paces anxiously) Wonderful. Okay, we need to act fast and smart. As a law firm, we have strict legal and ethical obligations here. We can't afford to bungle this. I'm calling an emergency meeting with our breach response team – that means you, me, our outside cybersecurity counsel, and our insurance lawyer. We must handle this by the book – complying with all laws **and** ethics rules. No mistakes.

(He picks up the phone and starts making calls to convene the team.)

Facilitator: *(to the audience)* Before we move on, let's pause the action for a moment and consider an important question about what **should happen first** in this situation.

[**Discussion Break**]

- **Facilitator:** "What should the firm do *first* after discovering a cyber breach?"
  A. Notify all clients of the breach immediately.
  B. Contain the breach (stop further data loss and secure systems).
  C. Contact law enforcement.
  D. Pay any ransom demand (if this was a ransomware attack).

(Allow the audience a moment to think or vote on their answers. After responses, the facilitator continues.)

- **Facilitator:** The best immediate step is to **contain and investigate the breach** (option B). In our skit, the IT Manager did exactly that by resetting passwords and taking servers offline. You generally shouldn't notify clients or authorities until you've contained the situation and at least preliminarily assessed what's going on — otherwise you might not have accurate information to report. Contacting law enforcement (option C) is often advisable, but usually after initial containment and in parallel with required notifications. And paying a ransom (option D) isn't a "first" step; it's a last-resort consideration in specific ransomware scenarios (not evident here). So, containment is the critical first move to protect client confidentiality and prevent further damage.

(Having discussed this, the facilitator resumes the skit.)

Scene 2: The Breach Response Team Emergency Meeting

Setting: The team has gathered in the firm's conference room for an emergency strategy meeting, minutes later. The Managing Partner and IT Manager are physically present. Outside Counsel and Insurance Counsel join via a video conference call (their voices audible in the room). On the conference table is a copy of the firm's **incident response policy** for each person… which turns out to be a very thin binder. A smart speaker with **Chat JD** (the AI assistant) is also set up on the table.

Managing Partner: Thank you all for jumping on this call so quickly. We have a confirmed data breach affecting sensitive client information. We need to discuss our response step-by-step: containment (which is underway), notification requirements, legal compliance under various laws, ethical duties to our clients, and anything else that comes up. I want to make sure we don't miss a thing.

IT Manager: I've also connected **Chat JD**, our AI legal assistant, into this meeting. You will see why we pay so much money for it. It can help answer technical legal questions on the fly. (Raises voice slightly) Chat JD, are you with us?

Chat JD: (cheerful) **Chat JD online!** Hello, team! I'm here and ready to help. Just ask if you need clarification or greater detail on any legal or ethical point. I'll do my best to assist - with only minor wisecracks.

Managing Partner: Great. Let's get started. First, IT Manager, you've contained the immediate breach, correct?

IT Manager: Yes, as I mentioned, I reset passwords and isolated the affected servers. The intruder's access has been cut off. I'm continuing to investigate exactly which files were compromised.

Managing Partner: Good. Containment is our first priority, and that's done. Now, what do we know about the scope of compromised data? That will drive our next steps, especially who we must notify.

IT Manager: Based on the early forensics, the attackers accessed:

- A network folder with clients' personal information including names, addresses, driver's licenses and Social Security and EIN numbers.
- Some financial account information related to client billing, bank account numbers and credit card numbers.
- Medical records we had on file for a personal injury case and medical practice patient identifier files provided as part of due diligence for the sale / purchase of medical practices (which is **Protected Health Information, or PHI**).
- And some case file documents that include attorney-client communications (privileged material).

So essentially, we have **"private information"** as defined by New York law, plus health/medical data PHI under HIPPA, and even some potentially privileged legal information all caught up in this breach.

Outside Counsel: Understood. That's a broad range of sensitive data. Let's tackle our legal obligations one category at a time. First up: the New York **SHIELD Act**, which governs breaches of "private information" for New York residents. The name "SHIELD" stands for "Stop Hacks and Improve Electronic Data Security." This law applies to any business that holds New York residents' private data – including law firms like ours. Under the SHIELD Act (N.Y. Gen. Bus. Law § 899-aa), if there's been unauthorized access to private information, we must notify the affected individuals **“in the most expedient time possible and without unreasonable delay.”**

Managing Partner: (nodding) So we can’t sweep this under the rug. We have to alert those clients or individuals whose data was stolen, as soon as we reasonably can.

Chat JD: If I may add — “without unreasonable delay” in practice means we should aim to notify quickly, generally **within 30 days of discovering the breach**. We can’t wait around for months. The only allowable reason to delay notification would be if law enforcement officially requests a delay to avoid impeding an investigation. We can’t delay just because we’re embarrassed or still figuring things out. The clock started ticking as of today when we discovered the breach.

Outside Counsel: Exactly. Thanks, Chat JD. We’ll need to start preparing breach notification letters immediately. Also, under the SHIELD Act, we have to notify certain state agencies. Since New York residents are impacted, we must alert the New York Attorney General’s office, as well as the state police and the Department of State. New York provides an online portal for reporting data breaches to those authorities. And if more than 5,000 New York residents were affected (unlikely for our firm’s size, but we should verify the number), we must also notify consumer credit reporting agencies of the breach.

Insurance Counsel: Right. We should check how many individuals’ data is involved. Even if it’s not 5,000, we’ll definitely be notifying the NYAG’s office. And here’s a critical point: if we fail to send out any required notifications, New York law can hit us with heavy penalties. I recall it’s up to **$20 per failed notification, up to $250,000** total for a single breach. And penalties for not having adequate security measures can be up to **$5,000 per violation** of the safeguard requirements. Our cyber insurance policy might *not* cover those fines if they result from us knowingly violating the law or our obligations. So, bottom line — we comply fully, and we do it fast.

Managing Partner: (grimacing) Ouch. Message received: we will notify everyone we need to. No hesitations.

IT Manager: I'll start compiling a list of all clients and individuals whose data was in the breached folders. We probably have dozens of New York clients' personal info involved.

Outside Counsel: Good. Now, the next category: those medical records mean we might be dealing with **HIPAA** obligations as well. The Health Insurance Portability and Accountability Act (HIPAA) protects medical information. Our firm isn't a hospital or doctor's office, so we're not a covered entity ourselves, but we likely received those medical records from a healthcare provider client (perhaps a hospital) as part of a case or transaction. That would make us a **Business Associate** under HIPAA for that client. We should have a **Business Associate Agreement (BAA)** on file with that hospital or healthcare entity.

Managing Partner: We do have a hospital client related to that case. I think they gave us a patient records release form. Isn't that the same thing as a Business Associate Agreement?

Outside Counsel: Not exactly. **Chat JD, can you clarify the difference between a patient release and a Business Associate Agreement?**

Chat JD: Certainly! *(in a helpful, explanatory tone)* **A Business Associate Agreement (BAA)** is a contract between a HIPAA-covered entity (like a hospital, medical practice or health plan) and a third-party service provider (the "business associate," which would be us, the law firm, in this case). The BAA contractually requires the law firm to safeguard protected health information (PHI) and to report any breaches to the covered entity. It basically ties us into upholding HIPAA rules and outlines our responsibilities and liabilities.

On the other hand, **a patient's HIPAA release form** (or authorization) is something a patient signs to allow their healthcare provider to release records to someone else – for example, to us, their lawyers. It's permission from the patient. **But it's not an agreement with us about how we will protect that information.** The BAA *is* that agreement about data protection between the firm and the hospital or the provider.

So, in short: the hospital client should have had us sign a BAA, which contractually obligates us to protect the PHI and to notify them if it's breached.

Managing Partner: Got it. So if we have PHI from the hospital, we're considered their "business associate" and we have to report this breach to the hospital under HIPAA rules.

Outside Counsel: Exactly. Under the **HIPAA Breach Notification Rule**, since we're a business associate that experienced a breach of PHI, we must notify that healthcare client (the covered entity) **without unreasonable delay and no later than 60 days** after discovering the breach. In practice, we'll notify them much sooner — as soon as we have a handle on what happened, likely within the next day or so. Then the hospital, as the covered entity, will be responsible for any further notifications to the affected patients, to the U.S. Department of Health and Human Services (HHS), and if the breach is large (more than 500 patients), to the media as well. We basically hand the baton to the hospital after informing them, but we need to give them enough information so they can fulfill their obligations.

Managing Partner: So, to be clear, we notify our client (the hospital) about the breach of their patients' data on our system, and then *they* will handle notifying the individual patients?

Outside Counsel: That's right. We'll tell the hospital immediately. They will handle the patient notifications as required by HIPAA. One thing to note: the New York SHIELD Act has an overlap provision. If we're already notifying individuals under another law like HIPAA, that can count as the individual notice under SHIELD Act. In other words, we don't have to send two separate notices to the same person for HIPAA and SHIELD. **However**, even if HIPAA covers the patient notifications, **we still have to notify the New York Attorney General's office about the breach**. SHIELD Act doesn't let us off the hook for notifying the state authorities just because it's health data. So no double-notifying the individuals, but we *do* need to make sure New York state knows about this incident as it involves New Yorkers' health info.

Insurance Counsel: And don't forget, the New York Attorney General can enforce HIPAA in some cases too. The Health Information Technology for Economic and Clinical Health Act or HITECH Act from 2009 – which was designed to incentivized use of Electronic Health Records (EHRs) - strengthened the privacy and security provisions of HIPAA. The HITECH Act is what extended the reach of HIPAA to business associates of covered entities and made them accountable for failures of HIPAA compliance. The Act also introduced tougher penalties for violations of HIPAA. Thanks to the HITECH Act, state AGs have authority to enforce HIPAA violations. So if we mishandle this PHI breach, we could face inquiries or penalties under HIPAA from the state level, not just federal. A bit of a double-whammy if we're not careful: SHIELD Act enforcement and HIPAA enforcement.

Managing Partner: (sighs) We will be very careful. Let's make sure to coordinate closely with our healthcare client on this. Perhaps we can even do a **joint notification** with the hospital – so they see we're handling it responsibly and transparently. I'll personally call the general counsel of the hospital as soon as we have the basics down, maybe even right after this meeting.

IT Manager: I'll segregate all the files that contained PHI and get you a list of exactly what patient data was involved and which patients. That way, Outside Counsel can draft our notice to the hospital with those specifics at hand.

Outside Counsel: Good plan. Now, beyond these statutory laws (SHIELD Act, HIPAA), we need to consider our **ethical duties as lawyers.** The New York Rules of Professional Conduct are very much in play during a cybersecurity incident like this.

Let's talk ethics: We know we have a fundamental duty of **confidentiality** under **Rule 1.6**. New York's Rule 1.6(c) explicitly states that *"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rule 1.6."*

Chat JD: (chimes in with a slightly dramatic tone) To put it plainly, Rule 1.6 requires us to **safeguard client information**. And, well, here we have an instance of unauthorized access that has already occurred despite our efforts. That suggests we might need to question whether our safeguards were "reasonable" as the rule requires.

Managing Partner: (rubbing temples) Right… Rule 1.6 basically says we have to take reasonable precautions against data breaches. And now we've had a breach. If it turns out we didn't do enough beforehand, we could be seen as having fallen short of our ethical duty to protect client confidences.

Outside Counsel: Correct. We'll have to assess later whether our security measures were up to snuff. For now, another ethical duty has kicked in — the duty to inform and communicate with our clients. Under **Rule 1.4 (Communication)**, we must keep clients reasonably informed about significant developments relating to their representation. A data breach that compromises their confidential information *definitely* qualifies as a significant development. Multiple ethics opinions (including ABA Formal Opinion 483) make it clear that if client data is breached, the lawyer must promptly inform the client of the breach.

Insurance Counsel: I'm familiar with ABA Formal Opinion 483 (2018). It basically says that lawyers have to inform current clients about a data breach that **materially** affects the client's information or interests. It ties this into both our duty of communication (Rule 1.4) and confidentiality. There's even a New York State Bar opinion from 2010 (NYSBA Op. 842) that said if a lawyer's online storage provider is hacked, the lawyer must notify any clients whose data was potentially compromised. So this has been the expected ethical standard for a while now.

Managing Partner: Either way — by law or by ethics — we have to notify our clients. We might as well operate under the strictest requirements and cover all bases. We'll comply with the legal notification laws, and also ensure every affected client hears directly from us about what happened.

Outside Counsel: Agreed. We should prepare clear, tailored **client notification letters** (or scripts for calls) for each client whose matters are affected. This is separate from the generic notice letters to individuals under the SHIELD Act. For example, we have at least one corporate client whose case files were accessed (the surgical center litigation files you mentioned). That client needs to be informed about the breach and how it might impact their case. Ethically, we need to explain what happened, what we are doing about it, and advise if it could affect the representation — say, if any privileged material might have been exposed to an adversary or could affect strategy. We have to reassure clients we're handling it, but also be candid about the situation.

Managing Partner: Speaking of privileged material… What about attorney-client privilege? Could this breach be seen as waiving privilege for the documents that were stolen? I'd hate for our client's sensitive litigation info to lose protection just because some hacker (unrelated to the case) grabbed it.

Chat JD: If I may? Good question. Generally, an unauthorized theft of data — like a hacker break-in — is not considered a voluntary or intentional disclosure by the client or by us, so it *shouldn't* waive the attorney-client privilege. It's akin to someone breaking into our office and stealing files; the courts don't usually say privilege was waived in such cases. We would argue it's an involuntary breach and we took reasonable steps to protect the data. So privilege is maintained. However, if any of those documents do surface in the wild or, worse, in the hands of an opposing party, we'd need to take action (like seeking court orders to claw them back and prevent their use). For now, our job is to keep the information as confidential as possible moving forward and, importantly, to notify the client about the breach. They have a right to know and they shouldn't be blindsided if something does come out.

Insurance Counsel: Keep in mind, even if privilege holds, a client could still claim we were negligent in safeguarding their data. They might say we breached our duty. That could lead to a malpractice claim or at least some very difficult conversations about our responsibility for any damage. We have to be prepared for that possibility.

IT Manager: (softly) I have to ask… did we do enough to protect this data in the first place? I mean, I set up basic firewalls, antivirus, passwords… but clearly, the hackers found a way in. I've been pushing for more security measures, but we hadn't gotten them all in place yet.

Insurance Counsel: You're raising a fair point. This goes to the **preventative** obligations under both law and ethics. The New York SHIELD Act doesn't just impose breach notification duties; it also requires that we implement "reasonable administrative, technical, and physical safeguards" to protect private information. It even gives examples: having a security program coordinator, conducting risk assessments, training employees in security, selecting service providers that safeguard data, etc. If we lacked those measures, the NY Attorney General could penalize us up to **$5,000 per lacking safeguard**, separate from the breach notification fines. That's the legal side.

Ethically, the duty of competence (Rule 1.1) for lawyers today includes a duty of **technological competence**. We must understand the risks of the tech we use and take appropriate security measures. There's commentary in New York and ABA opinions reinforcing that if we don't keep our cybersecurity practices up to par, we could be seen as not competently protecting client interests. Plus, Rule 5.1 (responsibilities of partners and managers) and Rule 5.3 (responsibilities regarding non-lawyer assistants) make firm leadership – like you, Managing Partner – responsible for ensuring that the firm has appropriate policies and supervision in place to protect client information. In plain terms, firm management must actively maintain good cybersecurity practices and oversee that staff (lawyers and non-lawyers alike) follow them.

Chat JD: I'll add one more ethics rule here: **Rule 1.15 – Safeguarding Property.** Usually we think of Rule 1.15 in terms of preserving client funds and property (like money in escrow). But analogously, client files and data are “property” that we hold for the client’s benefit. The principle behind 1.15 is that we must take care of anything of the client’s that is in our custody. In the digital age, that principle extends to protecting electronic client data. So if we failed to secure our clients’ documents and data, one could argue we didn’t adequately safeguard client property. It underscores our fiduciary responsibility to guard client information as diligently as we guard client funds.

Managing Partner: (looking chagrined) We did have security measures in place, but… clearly we could have been more thorough. (He glances at the IT Manager.) We were *planning* to roll out more secure systems – like that multi-factor (2FA) authentication – but we hadn’t done it yet.

IT Manager: (wincing) It was on my to-do list to enable multi-factor authentication and a new encryption routine for sensitive files next quarter. I guess the hackers didn’t get the memo to wait for our upgrade schedule.

Managing Partner: (half-smiles despite himself) Well, water under the bridge now. Let’s focus on fixing this.

We’ll **immediately** implement the security enhancements that were in the pipeline. Consider this our painful learning experience – our deadline for tech improvements just got moved up to “right now.”

Insurance Counsel: Good. We’ll definitely bolster our safeguards after we get through this crisis. Now, another angle: our **cyber insurance policy**. I’ve already notified our insurer first thing this morning that we have a potential claim. The policy usually covers a lot of the response costs for breaches – like hiring a forensic IT investigator, paying for credit monitoring for affected individuals, legal fees for breach response counsel (that's you, OC!), and even things like ransom payments or data recovery if it had been that kind of breach. But to get those benefits, we must strictly follow the policy's requirements, starting with **prompt notice** to the insurer. We've done that. The insurer will likely assign a claims specialist and pre-approve us to hire a forensic firm ASAP to investigate. Prompt notice keeps us in good standing with our coverage. If we had delayed notifying the insurer, we might have jeopardized our coverage.

Outside Counsel: Glad to hear it's in motion. Now, what about involving law enforcement? Given that financial information and personal identifiers were taken (which raises the risk of identity theft or fraud), it's often a good idea to notify law enforcement authorities. Under the SHIELD Act, when we notify the state Attorney General and state police via the breach portal, law enforcement is effectively being notified. We might also consider reaching out directly to our local FBI cybercrime unit or state police cyber task force. Not only can they investigate the attack, but having an official report could help if, say, individuals later become victims of identity theft – they'll know this breach was a source. Plus, showing we involved law enforcement demonstrates we're being proactive.

Managing Partner: I agree. We will involve law enforcement as appropriate. Once we file the required notice with the NY Attorney General's office, that will automatically loop in the state authorities. We can also separately contact the local FBI cybercrime division to report the incident. Importantly, from an ethics standpoint, sharing information with law enforcement for the purpose of rectifying the breach or catching the perpetrators is generally allowed — it's in the clients' interest to stop the criminals and protect their data. Rule 1.6 permits disclosures that are "impliedly authorized" to carry out the representation or to prevent harm, so I'm comfortable we can talk to the police or FBI about what happened without violating confidentiality.

Chat JD: Yes – that's a good point. We're not breaching confidentiality by seeking help. It's ethically permissible to give law enforcement the information necessary to investigate, as it's aligned with protecting our clients' interests.

IT Manager: I'll make sure to preserve all system logs, access records, and any other digital evidence so that forensic investigators or law enforcement can analyze them. I've already imaged the affected server drives so we have a snapshot of the system at the time of the attack. Nothing will be overwritten or lost from this point — we'll maintain a clear evidence trail.

Managing Partner: Excellent. Preservation of evidence is critical. Okay, let's recap our plan so far and see if we've missed anything:

1. **Breach contained** – thanks to IT's quick action.
2. **Notify authorities** – we will notify the NY Attorney General via the breach reporting portal, which covers the AG, state police, and Department of State. And we'll reach out to the FBI cyber unit.
3. **Notify our insurance carrier** – already in progress, thanks to Insurance Counsel, to ensure coverage and get resources like forensic experts.
4. **Notify affected individuals** – we'll send prompt breach notices to all individuals whose private information was compromised, as required by the SHIELD Act.

5. **Notify clients** – we will personally inform every client whose matters were impacted, in line with our ethical duties (and contractual duties, like the BAA for the hospital client).
6. **Notify the healthcare client** – the hospital gets a special notice from us about the PHI breach, so they can handle patient notifications under HIPAA.
7. **Mitigation for victims** – we should offer credit monitoring or identity theft protection to individuals whose personal data (SSNs, financial info) was stolen. It's not explicitly mandated by NY law, but it's a best practice and shows good faith. Our cyber insurance should cover the cost of, say, a year of credit monitoring for each affected person.
8. **Remediation and future prevention** – we will develop a plan to improve security (implementing encryption, multi-factor auth, training staff, etc.) to meet the SHIELD Act's "reasonable safeguards" requirements and to fulfill our ethical obligation to prevent this from happening again.

Did I miss anything in that list?

Outside Counsel: That's a pretty comprehensive list. One more item: **communications and transparency**. We should coordinate any public relations or media response, in case the story gets out (especially since breaches involving personal data can become public via the Attorney General's reports or if any notification letter leaks). Under the ethics rules, specifically Rule 8.4 (which prohibits dishonesty, fraud, deceit, and misrepresentation), and in general our duty of candor, we must make sure that any communications about the breach are truthful. We can't spin this by hiding key facts or lying. So our notifications and any statements should be candid about what happened, what we're doing, without unnecessary technical jargon or deflection. Of course, we don't need to include *every* detail (like exactly which employee got phished – no need to throw anyone under the bus), and we should avoid speculation. But overall, honesty is critical.

(smiles wryly) And perhaps avoid too much humor in the official communications — a little empathy and apology goes a longer way than trying to make a joke. We'll save the jokes for our internal CLE skits.

Managing Partner: (cracks a slight grin) Noted. Our breach notification letters will be serious and apologetic in tone. No "LOL we got hacked, our bad!" messaging. We'll strike a professional, transparent tone.

Insurance Counsel: Speaking of plans and checklists, maybe we should see how our response stacks up against a standard **Incident Response Plan**. Chat JD, do you have a generic incident response checklist we can cross-reference?

Chat JD: Absolutely. I have a model Incident Response checklist here. Let's compare our actions to the recommended steps:

- **Detect and Verify the incident:** ✓ Done. Our IT Manager noticed unusual activity and verified it was a breach. We didn't ignore the warning signs – we caught it early.
- **Contain the incident:** ✓ Done. We isolated affected systems and changed passwords to stop the bleeding.
- **Assemble the response team:** ✓ Done. Managing Partner immediately pulled together IT, Outside Counsel, Insurance

Counsel – a multidisciplinary team. (Gold star for fast assembling, by the way!)

- **Notify internal stakeholders:** ✓ Done. Firm management is in the loop. The key partners are all aware. No one's hiding this internally.
- **Engage outside experts as needed:** ✓ In progress. We have Outside Counsel here. Insurance is getting us a forensic firm. We'll likely involve an IT forensics vendor soon via insurance, and we've discussed law enforcement.
- **Assess legal obligations:** ✓ Done. That's been a big part of this meeting – SHIELD Act, HIPAA, ethics, etc. We know who we have to notify and by when.
- **Develop a communication plan:** ✓ Done. We are preparing notifications to clients, affected individuals, regulators, and even considering PR. We know what we'll say and how.
- **Notify external parties:** (Almost done) We've notified insurance. Next steps immediately after this meeting: send out notices to the AG and affected individuals, and call the clients.
- **Document everything:** ✓ Being done. IT is preserving logs and evidence. We'll document our investigation and response actions thoroughly – this meeting's decisions are being noted. All of this will go into a post-incident report.
- **Post-incident follow-up and remediation:** (Planned) We've already planned to upgrade security measures, do training, and create a robust formal incident response plan for the future. We'll make sure to follow through on those improvements.

Looks like you've checked almost all the boxes. In short, the firm's response is hitting all the major steps it should. Nicely done (given the circumstances)!

Managing Partner: (exhales with a bit of relief) That is reassuring to hear. It's a terrible situation, but we're doing everything we're supposed to do in response.

(The team members exchange determined looks, feeling more confident that they have a handle on the immediate next steps.)

[**Discussion Break**]

Facilitator: *(to audience)* Let's pause here for another quick discussion. The firm has addressed many issues simultaneously — but what would you say is their **highest priority** in responding to this breach?

A. Stopping further data loss and protecting client confidentiality.
B. Complying with legal obligations (notifications to clients, AG, etc.).
C. Protecting the firm's reputation.
D. Informing clients promptly about the breach.

(Take responses from the audience. Then the facilitator continues.)

- **Facilitator:** In a breach, several priorities must be managed in parallel, but if we rank them, the **first priority is to protect client confidentiality by stopping the breach (A)**. That means containing the incident to prevent any more data from leaking — which DCH did immediately. Next, **complying with the law (B)** and **informing clients (D)** are both critical and in fact go hand-in-hand: the law (like the SHIELD Act and HIPAA) requires notifying affected individuals and authorities, and ethics require informing clients. So the firm is doing both, as we've seen. **Protecting the firm's reputation (C)** is a consideration, but it should never overshadow the legal and ethical duties. In truth, the best way to protect reputation is by handling the breach responsibly (not by covering it up). In our story, DCH's leadership recognized that being transparent and diligent is the only way to respond.

(Having discussed these priorities, the facilitator cues the skit to continue.)

Scene 3: Client Notification and Aftermath

Setting: Later that day, in the same conference room. The team has spent a few hours drafting the necessary notification letters and emails. The Managing Partner has decided to personally call one of the firm's major clients — a corporate client — whose sensitive data was involved, to inform them before any written notice goes out. The Client, Bob Major, CEO of Hospital for Misadventures is on speakerphone; the Managing Partner, IT Manager, Outside Counsel, and Insurance Counsel are gathered around. *(Chat JD is temporarily muted during this client call — the firm opts for a human touch when talking to clients.)*

Managing Partner: (speaking into the phone) Hello, Mr. Major? I'm glad I reached you. It's Cani Cheatum the Managing Partner from Dewey Cheatum & Howe. I…I have some serious news to share, and I wanted to call you personally as soon as possible. Our firm suffered a data breach over the weekend. Unfortunately, some of your company's information on our servers was accessed by an unauthorized intruder. The breach has been contained, but I want to walk you through what happened and what steps we're taking.

Client (on phone): (voice of concern) Oh no… That's really alarming to hear. What information of ours was compromised?

Managing Partner: Our investigation is ongoing, but it appears that some of your files were accessed. Specifically, the files related to the **Surgical Center litigation** we're handling for you — those included some of you're the Hospital's financial records you provided to us, and correspondence and documents from that case, which are protected by attorney-client privilege. To be clear, at this stage we don't have evidence that the data was leaked publicly or misused beyond the hacker's intrusion. It seems the breach was a random cyberattack, not specifically targeting the Hospital. But we felt it was crucial to alert you immediately, even as we continue to gather details.

Client: This is very disappointing, to put it mildly. We trusted your firm to keep our information safe. I understand cyberattacks happen, but I need to know: what obligations do we have now, and are we exposed legally because of this breach? For instance, if our patients' or employees' info was in those files, do we have to notify them? And could this breach impact our ongoing litigation?

Outside Counsel: (clearing throat, speaking reassuringly) Hi Mr. Major, this is Perry Mason. I'm outside counsel assisting DCH with the legal response to this incident. From what we know, some of your data in our possession was compromised, so let me address your concerns one by one.

First, in terms of legal obligations: **DCH is taking care of all necessary notifications.** Under New York's SHIELD Act, if any personal data (like individuals' names coupled with social security numbers or financial account numbers) was involved, DCH will send out the required breach notices to those individuals on your behalf, since the breach occurred on our systems. We will also be notifying the New York Attorney General's office about the incident, as required by law. Essentially, we're handling the compliance steps that relate to the data that was in our custody.

If any of the data in those case files involves just personal information of your patients or employees (for example, if we had a list of your employees with their contact info or SSNs as part of discovery documents), we will absolutely coordinate with you on notifying them. We want to ensure no one is left in the dark. But legally, the duty to notify for this breach lies with us, the law firm, since it was our system that was breached. You won't have to personally send out notifications, though we'll keep you in the loop on everything we do.

If any of the data in those case files involves PHI personal health information of your patients or employees DCH is a business associate, and will follow HIPAA's breach requirements. That means beyond this notification today DCH will, without unreasonable delay and in no event later than 60 from today provide you with the names, contact information and PHI accessed so Hospital for Misadventures can fulfill its obligations by notifying the affected patients, HHS, and if the number is greater than 500 people, the media. Although not required, DCH has of course voluntarily elected to work with the Hospital and provide the necessary notices.

Client: So DCH will cover all of our costs and expenses for any notices that must be given?

Managing Partner: We will work with you and our insurance carrier and provide the notices at our cost.

Outside Counsel: As for your ongoing litigation — I know that's a big worry, especially if privileged communications were accessed. The good news is, the hackers appear to be cybercriminals with no connection to the opposing party in your case. We have no indication that any litigation adversaries have seen the information. So this breach *should not* impact the litigation directly. Attorney-client privilege still stands; it isn't waived just because some outsider stole the documents. We consider those documents still confidential and privileged.

Client: And what if, worst-case scenario, those privileged documents somehow get out in the world?

Managing Partner: If any of the stolen information were to surface or be misused in a way that threatens your interests, our firm would take immediate action. For example, if any privileged documents appeared somewhere they shouldn't, we'd go to court to seek an order to protect that information (to prevent anyone from using it against you) and to have it returned or destroyed. We are committed to doing everything possible to make sure this breach does *not* hurt your legal position.

Also, I want to emphasize: we feel terrible that this happened. Under our ethical rules, we have a duty of confidentiality to you, and part of that duty is to inform you when something goes wrong. That's why we’re being completely transparent now. We take that obligation very seriously — we’re treating this as if our own sensitive information were at stake, because that’s how important our clients’ trust is to us.

Client: I appreciate the transparency and the quick call. This gives me some initial comfort that you’re on top of it. But I’m still very concerned. What is DCH doing to fix this problem and ensure it never happens again? I need to know that our data will be safe going forward if we continue our relationship.

IT Manager: (speaking earnestly) Those are absolutely valid concerns. Please know, we are already working on bolstering our systems. We aren’t waiting. Concretely, here’s what we’re doing immediately:

- We are implementing **stronger encryption** for all stored data, so even if someone gets in, the files would be encrypted and unreadable without proper keys.
- We are turning on **multi-factor authentication** for all access to our network and services whether accessed by computer or handheld device. That means even if someone somehow learns a password, they still can’t get in without a secondary verification (like a code from a phone). This greatly reduces the chance of a single phishing email leading to a breach.
- We’re enhancing our **network monitoring** and alert systems so that any unusual activity is caught and flagged even faster, hopefully preventing incidents before they escalate.

Frankly, these are measures we were in the process of rolling out — this incident just turned them into an urgent priority. We’re also scheduling firm-wide cybersecurity training for all our attorneys and staff to help everyone recognize phishing attempts and other threats. (In fact, cybersecurity awareness training is now *mandatory* for New

York lawyers as part of their CLE requirements, so we'll be taking advantage of that to improve our human defenses, not just the technical ones.)

Insurance Counsel: To add to that, as part of our remediation and client care, DCH is activating resources through our cyber insurance. For any of **your** employees or patients whose personal data might have been involved via those files, we will provide them with complimentary credit monitoring and identity theft protection services for a substantial period (typically 1 year). Our insurance will cover the cost. This is both a goodwill gesture and a protective measure. It ensures that if, say, a Social Security number or financial account from your files was in the breached data, those individuals will be alerted to any signs of identity theft and have support to resolve it. We want to minimize any harm that comes from this incident.

Client: That's good to hear. It sounds like you're addressing the immediate damage and also beefing up your defenses. Now, regarding regulators or any official reports — do I, as the client, need to do anything on that front? For instance, if our data was involved, would our company need to notify anyone or file any reports? What about the PHI?

Outside Counsel: In this case, because the breach occurred within the law firm's environment, DCH is taking responsibility for all required notifications. We will be filing the necessary notice with the New York Attorney General's office and other relevant state bodies. The Hospital will not have a direct obligation to notify regulators about this incident since it didn't happen in your systems. As for the PHI even though the Hospital has the obligation under HIPPA to give your patients the notification, DCH will also handle any HIPAA related notifications, as we discussed. That said, we will coordinate closely with you. For example, we'll share copies of the notification letters that go out, and if any of the data overlaps with your obligations (though I think it's mostly on us), we'll make sure everything is covered. If you get any inquiries (say, if one of your employees hears about it and contacts you), you'll have the information at hand to respond. Legally, though, DCH is the entity that was breached, so DCH will handle the formal reporting**.**

Managing Partner: Bob, I want to personally apologize again for this incident. We deeply value the trust you placed in us as your legal counsel. Protecting your confidential information is fundamental to our profession and our relationship with you. We are determined to make this right. We will send you a detailed follow-up letter outlining everything we discussed — what happened, what data we believe was involved, what we've done so far, and what we will do going forward. That letter will also include a direct contact at our firm (and at the credit monitoring service) for any questions or support you or your team might need.

We will work with you and your team in connection with all required notices to assure that we have complied with all legal requirements.

Also, please know that we fully intend to cover any reasonable costs that you or your employees incur because of this breach. Our insurance is meant for exactly this kind of situation. And beyond the letter, we'll keep you updated at every major development. If we discover more in our investigation that affects you, you'll hear it from us right away. You shouldn't have to chase us for information — keeping you informed is our duty (and frankly, the only way to maintain your trust).

Client: Thank you. I am, of course, upset that this happened, but I do appreciate the swift action and the direct communication. This kind of honesty is what I expect. We will review the written notice when it comes. And yes, I will expect that DCH will take care of any costs or damage that results — it sounds like you will. We will also need to have a discussion soon about what steps you're taking to prevent this in the future, because I need to be confident it won't happen again if we continue working together.

Managing Partner: Absolutely. Once we get through the immediate response, I'd like to set a meeting with you (maybe in the next week or two) to go over the enhanced security measures we're implementing. We want you to be fully comfortable with how we'll be protecting your information going forward. Rebuilding your trust is critically important to us.

Client: Okay. This is certainly a wake-up call. I'll look for your letter and the credit monitoring details. In the meantime, if you need anything from us, let me know. I'll inform a couple of key people on my team about this, but we'll keep it internal on our side unless there's a need to disclose it. Let's talk again soon once more information is available.

Managing Partner: That sounds good. Thank you for your understanding, [Client Name]. We will talk soon, and please don't hesitate to reach out with any questions in the meantime.

Client: Will do. Thanks.

(The Client hangs up. The conference room falls quiet for a moment as the team exhales collectively.)

IT Manager: (quietly) Well, that was intense.

Insurance Counsel: That went about as well as we could hope. The Hospital is understandably upset, but they appreciated the transparency and swift action. In breach situations, being forthright is crucial. If we had tried to hide this or downplay it, the outcome could have been far worse — both in terms of trust and potential legal consequences.

Chat JD: I was listening and thought that you addressed the legal and ethical issues. Remember, many ethics experts emphasize that hiding a breach is not an option. In fact, as was discussed earlier, ABA Formal Opinion 483 basically mandates that lawyers must inform clients of a data breach that impacts the client's information. We've done exactly what we're supposed to: notify promptly, explain what happened, and outline how we're fixing it. Ethically and legally, that's the right call.

Managing Partner: I agree - I'm agreeing with a computer - I hated making that phone call. No one wants to tell a client bad news but it was our duty and ultimately it helps preserve the relationship by showing we take this seriously. Now, looking ahead, we need to make sure we follow through on everything we promised. That means implementing the robust **Incident Response Plan** we frankly should have had in detail before now, and strengthening our security across the board.

(He picks up the thin incident response policy binder on the table and gives a wry smile.)

Remember this so-called incident response plan? It's basically a skeleton. (He flips through near-empty pages.) That's going to change. We are going to develop a comprehensive plan, in writing, and train everyone on it, so if anything like this ever happens again, we're even more prepared.

Chat JD: In Formal Op. 483 and other guidance, there's a strong suggestion that having an incident response plan **in advance** is part of being competent in cybersecurity.

Managing Partner: We've learned that the hard way. Not having a solid plan could itself be seen as a lapse in our duty to safeguard client data. Well, consider the lesson learned.

IT Manager: I'll draft a full **post-incident report** documenting everything: how the breach happened, all the steps we took in response, and what we're going to improve. That documentation will be useful if any regulators inquire, and it will serve as a roadmap for our remediation steps.

Managing Partner: Good. We'll also schedule an all-hands firm meeting to go over new security policies and training. Every attorney, paralegal, and staff member needs to understand their role in protecting data — from using strong passwords to being able to spot phishing emails. This incident is going to become a case study in our next training session (anonymized, of course). At least New York now mandates attorneys take cybersecurity CLE, so we have an extra incentive to educate everyone. We'll turn this breach into something our whole firm learns from.

Outside Counsel: Excellent plan. And one more thing: we should not forget any **former clients** whose data might have been affected. Our ethical obligations to *current* clients are paramount (and we've addressed those), but if any old case files for former clients were in that breached data set, it's a best practice to inform them too. They may not be actively represented by us now, but they would certainly want to know if their confidential information from when we did represent them has been compromised. Many in the legal ethics community suggest notifying former clients in such a scenario, even if the rules on that are not explicit. It's about maintaining trust in the profession.

IT Manager: I saw a couple of closed matter files in the accessed folders.

Managing Partner: Agreed. We will absolutely reach out to those former clients with a courteous heads-up. It's the right thing to do. No client — current or former — likes finding out later that their data was breached while in our custody. We're not legally mandated to inform former clients in every jurisdiction, but ethically, it aligns with our duty of honesty and professionalism to let them know. So we'll do it.

Managing Partner: I have to say, team: It's been an incredibly challenging day, but thank you all for your quick and thorough action. This breach had the potential to be a disaster for the firm — even a career-ender — but I think we're turning it into a situation we can manage and learn from.

Chat JD: Reviewing the actions today DCH acquitted itself well. We contained the damage swiftly, we're complying with the SHIELD Act, HIPAA, and all other legal requirements, we upheld our ethical duties by informing our clients promptly, and we're setting ourselves on a path to be much stronger on security in the future.

Insurance Counsel: And with all the improvements we're going to implement, if (heaven forbid) something like this ever happens again, we'll be far better prepared. In essence, we're going to earn that "SHIELD" in the SHIELD Act. We might even end up like a little band of cybersecurity avengers for our firm. (Grins) "Agents of S.H.I.E.L.D.," legal edition, right?

IT Manager: (laughs) If so, I dibs the Nick Fury role — I've got the battle scars from this hack to prove it. Though I'd rather not collect any more scars any time soon.

Managing Partner: (chuckles) As long as I don't have to wear a cape or spandex, I'm on board. Jokes aside, let's formalize a simple mantra for our firm: **Prevent, Detect, Respond, Notify, and Remediate.** Those are the pillars of handling cybersecurity. We'll be drilling those into our procedures. We will put this in writing in our new incident response plan and make sure everyone at the firm knows the drill.

Chat JD: Yes, as to everyone knowing the drill we should make sure that the firm conducts a practice drill or tabletop exercise annually to review the steps that need to be taken and make sure the incident response plan is addressing the ever expanding cybersecurity issues. For instance, who knew 1 year ago that you would be using such a valuable AI resource!

Outside Counsel: All good points. In summary, this experience, while painful, has been educational for all of us. The key takeaway is that when a breach happened, the firm responded appropriately: you didn't hide it, you addressed all the legal notification requirements, and you put the clients' interests first at each step. That's exactly what both the law and our ethical rules require in such a situation. Not to mention, it's the best way to preserve your reputation and client relationships in the long run.

Managing Partner: Well said. I'm proud (in the end) of how we handled a bad situation. Of course, we'll keep fine-tuning our response as we learn more — for instance, if the forensic analysis reveals exactly which files were accessed or if any data was definitely exfiltrated, we may need to send follow-up notices or take additional steps. But big picture: we can confidently tell our clients, regulators, and yes, even the press if it comes to that, that we did everything required of us — and then some — to respond to this breach responsibly.

Chat JD: The firm will emerge from this with a stronger security posture. In conclusion, the firm is implementing a comprehensive breach response and prevention plan. We've taken our obligations under the NY SHIELD Act, HIPAA, and the Rules of Professional

Conduct with the utmost seriousness. This incident prompted us to shore up our defenses and procedures, which ultimately will better protect our clients and uphold the integrity of our profession. It's been a hard lesson, but a valuable one.

Managing Partner: That computer is going to take everyone's job! Thank you, everyone, for your hard work and candor throughout this ordeal. Now, let's finish up those notification letters and get them out the door. After that, we'll reconvene next week to review our new cybersecurity measures in detail and ensure they're all implemented.

Who knows, maybe someday we'll be invited to share this story as part of a CLE program to help other lawyers learn from our experience. At least if that happens, it will have a reasonably happy ending and a lot of useful lessons.

Outside Counsel: (laughs) Count me in if you do. This has been quite a fire-drill — nerve-wracking but ultimately instructive. Next time, let's run a planned simulation rather than live it for real!

Managing Partner: Deal. Thanks again, everyone. Let's get to work on the follow-ups, and hopefully enjoy a *quiet* remainder of the week after this storm.

End of Skit

[**Discussion/Q&A with Participants**]

Facilitator (to audience): Let's reflect on how the firm handled this incident:

- **Legal compliance:** How well did Dewey Cheatum & Howe comply with laws like the SHIELD Act and HIPAA? What steps did they take to meet those requirements, and were there any they almost overlooked?
- **Ethical obligations:** Did the firm fulfill its ethical duties under the NY Rules of Professional Conduct (Rules 1.1, 1.4, 1.6, 1.15, 5.1, 5.2, 5.3)? For example, how did competence and communication come into play? What about the role of firm management and staff training in preventing breaches?
- **Incident response best practices:** The skit showed an incident response in action. What did the firm do well in responding to the breach? Is there anything you might have done differently? What additional steps (if any) would you include in your own firm's incident response plan?
- **Prevention and preparedness:** This story underscores the importance of being prepared *before* a breach. What proactive measures (like policies, training, or insurance) can law firms put in place to mitigate the risk of cyber incidents or lessen their impact? How does planning (or lack thereof) affect the outcome?

(Allow participants to share thoughts on these questions. The panel can then highlight key takeaways, such as the value of quick containment, the necessity of candor with clients, the interplay of legal requirements and ethical duties, and the critical importance of having an incident response plan and robust security measures in place. End the session with a reminder that with proper preparation and ethical conduct, a law firm can survive a cyberattack and maintain client trust.)

NAVIGATING THE DATA BREACH MINEFIELD: A NEW YORK LAWYER'S ETHICAL AND LEGAL IMPERATIVES

Introduction

The legal profession, entrusted with highly sensitive information, faces an ever-escalating barrage of cyber threats. Data breaches targeting law firms are no longer isolated incidents but represent a significant and growing concern within the legal community. Statistics reveal an alarming trend in the frequency and severity of these attacks, highlighting the urgent need for lawyers to understand and address their responsibilities in this evolving landscape. Law firms are particularly attractive targets for cybercriminals who seek to exploit the vast repositories of personal, financial, and privileged information they maintain. These malicious actors often perceive law firms as possessing less robust security infrastructures compared to other industries like finance or healthcare, making them potentially easier targets. This perception is supported by the increasing number of reported data breaches affecting law firms, underscoring the reality of this threat.

Recent years have witnessed numerous high-profile data breaches impacting law firms, demonstrating the diverse nature of compromised data and the significant repercussions for the affected firms and their clients. Cases involving firms like Allen & Overy, Kirkland & Ellis, and the American Bar Association illustrate that even large and well-established organizations are susceptible to sophisticated cyberattacks. The types of data exposed in these breaches range from basic login credentials to highly sensitive client information, including personal identifiers, financial details, health records, and confidential attorney-client communications. The aftermath of these incidents often includes operational disruptions, substantial financial losses, and potential legal repercussions, further emphasizing the critical need for proactive security measures and effective breach response strategies.

In this digital age, a lawyer's ethical responsibilities extend beyond traditional notions of client confidentiality to encompass the proactive safeguarding of client data in electronic form. The fundamental duty of confidentiality, as enshrined in New York Rules of Professional Conduct (NY RPC) Rule 1.6, not only prohibits the knowing disclosure of client confidences and secrets but also mandates that lawyers make reasonable efforts to prevent the unauthorized access or disclosure of such information. The evolving technological landscape necessitates a proactive stance on confidentiality, requiring lawyers to continuously understand and implement appropriate security measures to protect client information within the digital environment. This proactive duty is further emphasized by various ethical opinions addressing the security of client data in cloud storage, email communications, and on mobile devices.

Furthermore, the duty of competence, as outlined in NY RPC Rule 1.1, now encompasses an understanding of the benefits and risks associated with technology used in legal practice. The commentary to this rule underscores the need for lawyers to stay informed about technological advancements relevant to their practice, including understanding cybersecurity risks and implementing appropriate safeguards. Ethical opinions have further clarified the importance of technological competence in areas such as e-discovery and cloud computing, reinforcing the notion that lawyers must possess a foundational understanding of the technologies they utilize to serve their clients competently.

Beyond these core ethical duties, it is paramount for lawyers to adopt proactive measures to protect client data and maintain the trust that is fundamental to the attorney-client relationship. Clients entrust their lawyers with highly sensitive information, expecting it to be handled with the utmost confidentiality. A data breach not only exposes this sensitive information but can also severely damage client trust, potentially leading to legal malpractice claims and reputational harm for the law firm. Therefore, a commitment to robust cybersecurity practices is not merely a matter of compliance but an essential element of fulfilling a lawyer's ethical and professional obligations.

1: UNDERSTANDING THE LEGAL FRAMEWORK

A. The New York SHIELD Act: Key Provisions and Obligations for Law Firms

The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act represents a significant strengthening of New York's data security laws, imposing crucial obligations on any person or business that maintains private information of New York residents, including law firms. A key aspect of the SHIELD Act is its expansion of the definition of "private information" beyond the scope of the previous 2005 law. This now includes biometric information such as fingerprints or voice prints, as well as a username or email address in combination with a password or security question and answer that would permit access to an online account. This broadened definition means that law firms must consider a wider array of data elements as protected "private information" when handling typical client data such as driver's licenses, social security numbers, and financial account information, as well as these newer forms of digital identifiers.

Furthermore, the SHIELD Act significantly alters the threshold for triggering a data breach notification. The previous law defined a breach as an "unauthorized acquisition" of computerized data that compromised the security, confidentiality, or integrity of private information. The SHIELD Act expands this definition to include any "access" to computerized data that compromises the confidentiality, security, or integrity of private data. This shift from acquisition to access lowers the threshold for what constitutes a data breach, requiring law firms to be more vigilant in monitoring access to their systems and potentially leading to more frequent notification obligations even in the absence of evidence that the data was copied or misused.

A cornerstone of the SHIELD Act is its mandate that any person or business maintaining private information, including law firms, must develop, implement, and maintain "reasonable safeguards" to protect the security, confidentiality, and integrity of that information. The Act outlines three categories of these safeguards: administrative, technical, and physical. Reasonable administrative safeguards include measures such as designating an employee to coordinate the security program, identifying foreseeable internal and external risks, assessing the effectiveness of existing safeguards, training employees in security procedures, selecting capable service providers and requiring contractual safeguards, and adjusting the security program as needed. Technical safeguards involve assessing risks in network and software design, information processing, transmission, and storage, as well as implementing measures to detect, prevent, and respond to attacks or system failures, and regularly testing and monitoring security effectiveness. Finally, reasonable physical safeguards include assessing risks of information storage and disposal, preventing intrusions, protecting against unauthorized access, and ensuring secure disposal of private information. This requirement necessitates a proactive approach to data security, compelling law firms to assess their specific risks, implement tailored controls, and continuously review and update their security measures to remain compliant.

In the event of a data breach affecting private information, the SHIELD Act imposes specific notification requirements. Law firms are obligated to notify affected clients (present and former) in the most expedient time possible, consistent with the legitimate needs of law enforcement agencies. This notification must include details about the breach, the type of data affected, steps individuals can take to protect themselves, and contact information for inquiries. The law also requires notification to the Office of the New York State Attorney General (NYAG), the New York Department of State (DOS), and the New York State Police regarding the timing, content, and distribution of the notices and the approximate number of affected person. Recent amendments to the data breach notification law, effective December 21, 2024, have introduced a specific 30-day deadline for notifying affected individuals. Additionally, certain entities regulated by the New York Department of Financial Services (NYDFS) now have a separate obligation to notify NYDFS of a breach. If a breach affects more than 5,000 New York residents, notification to major consumer reporting agencies is also required. These stringent notification obligations underscore the importance of prompt and accurate reporting in the event of a data breach.

Failure to comply with the SHIELD Act can result in significant penalties. For failure to provide timely notification, a court may impose a civil penalty of up to $20 per instance of failed notification, not to exceed $250,000. Moreover, failure to maintain reasonable safeguards can lead to a civil penalty of up to $5,000 per violation. These substantial penalties underscore the critical importance of both implementing and maintaining reasonable safeguards to prevent data breaches and adhering to the notification requirements when a breach does occur.

B. HIPAA Compliance for Lawyers: When Does it Apply?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes specific obligations on "covered entities" – which include health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically – as well as their "business associates". Law firms typically fall under the definition of a business associate when they perform certain functions or activities on behalf of a covered entity that involve the use or disclosure of

"Protected Health Information" (PHI). This often occurs in legal matters such as medical malpractice litigation, personal injury cases, workers' compensation claims, and family law cases involving medical records, where access to client medical information is necessary to provide legal representation.

"Protected Health Information" (PHI) is broadly defined as any individually identifiable health information held or transmitted by a covered entity or its business associate in any form, whether electronic, paper, or oral. This encompasses a wide spectrum of medical and health-related data that law firms may encounter in their practice, including patient names, addresses, medical histories, diagnoses, treatment information, and insurance detail.

Under HIPAA, law firms acting as business associates are directly liable for complying with the HIPAA Privacy, Security, and Breach Notification Rules. To ensure compliance, covered entities must enter into Business Associate Agreements (BAAs) with their business associates. These agreements outline the specific responsibilities of the business associate in safeguarding PHI and detail the procedures for reporting breaches of unsecured PHI to the covered entity.

In the event of a breach of unsecured PHI, HIPAA mandates specific notification requirements for business associates. A business associate must notify the covered entity of the breach without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. This timely notification enables the covered entity to fulfill its own obligations under HIPAA, which include notifying affected individuals, the U.S. Department of Health & Human Services (HHS), and, in certain circumstances involving breaches of over 500 individuals, prominent media outlets. While it is less common, if a law firm itself meets the definition of a covered entity (e.g., by providing certain healthcare services), it would have direct notification obligations under HIPAA.

C. New York Rules of Professional Conduct: Core Ethical Duties in the Context of Data Security

The New York Rules of Professional Conduct Part 1200 establish the ethical standards governing the conduct of lawyers in New York State, and several rules are particularly relevant in the context of data security and data breaches. Rule 1.1, addressing competence, mandates that a lawyer should provide competent representation to a client, which now includes maintaining technological competence relevant to the lawyer's practice. This requires lawyers to understand the benefits and risks associated with technology used to provide services to clients or to store or transmit confidential information.

Rule 1.4, addressing communication, imposes a duty on lawyers to inform clients about material developments in a matter. A cybersecurity incident that compromises, threatens to compromise, or prevents a lawyer from accessing client confidential information constitutes a material development that must be promptly communicated to current clients. This communication should include sufficient information about the nature of the breach, the types of data involved, the steps taken to address it, and any potential mitigation measures the client may need to undertake.

Rule 1.6 is central to a lawyer's ethical obligations regarding data security, as it governs the confidentiality of information. This rule prohibits a lawyer from knowingly revealing confidential information or using it to the disadvantage of a client, unless an exception applies, such as client consent or as permitted by other provisions of the rule. Importantly, Rule 1.6(c) explicitly requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by the rule. This obligation necessitates the implementation of reasonable security measures to safeguard client confidences and secrets in the digital environment.

Rule 1.15 addresses preserving the identity of funds and property of others, emphasizing fiduciary responsibility. While primarily focused on financial assets, the principle of safeguarding client property extends to ensuring the security and integrity of client data stored electronically. The fiduciary duty inherent in the attorney-client relationship requires lawyers to protect all forms of client property, including digital files containing sensitive information, from loss, unauthorized access, or misuse.

Finally, Rules 5.1, 5.2, and 5.3 delineate the responsibilities of law firms, partners, managers, supervisory lawyers, and nonlegal assistants in ensuring the firm has policies and procedures in place to protect client information. These rules place an ethical obligation on law firms and those in supervisory roles to establish and maintain internal policies and procedures designed to safeguard client confidential information, including the implementation of reasonable cybersecurity measures and ensuring compliance by all firm personnel, both legal and nonlegal.

D. Overview of Relevant New York Ethical Opinions

Several New York State Bar Association (NYSBA) and New York City Bar Association (NYC Bar) ethics opinions provide further guidance on a lawyer's ethical obligations in the context of data security.

NYSBA Ethics Opinion 842 addresses the use of online data storage systems for client confidential information. This opinion concludes that lawyers may utilize cloud storage, provided they exercise reasonable care to ensure the system is secure and that client confidentiality is maintained. This includes diligently investigating the data storage provider's security measures, policies, and recoverability methods, and staying abreast of technological advancements and potential risks.

NYC Bar Formal Opinion 2024-3 offers comprehensive guidance on the ethical obligations of lawyers and law firms in the event of a cybersecurity incident. This opinion addresses various crucial aspects, including the fundamental obligation to take appropriate steps to protect clients' confidential information, the ethical duty to promptly notify current clients under Rule 1.4 when a cybersecurity incident occurs that constitutes a material development, considerations regarding ransom payments, and the ethical implications of disclosing client confidential information to law enforcement or in connection with a government investigation.

In addition to these key opinions, other NYSBA and NYC Bar ethics opinions address specific aspects of data security, email communication, and technology use.

These opinions cover topics such as protecting client identity information on smartphones, the ethical considerations of using cloud data storage tools for sharing documents, a lawyer's ethical duties regarding U.S. border searches of electronic devices containing client confidential information, and the obligation to notify clients of a data breach involving an online cloud data storage provider. These opinions collectively highlight the ongoing effort by the bar associations to provide lawyers with relevant and timely ethical guidance in response to the rapidly evolving technological landscape and the persistent threat of cybersecurity incidents.

2: IDENTIFYING THE THREATS AND VULNERABILITIES

A. Common Data Breach Scenarios in Law Firms: How Hackers Gain Access

Law firms face a multitude of cyber threats that can lead to data breaches. Phishing and social engineering attacks remain highly prevalent methods used by cybercriminals to gain unauthorized access to sensitive information. These attacks often involve deceptive emails, messages, or websites designed to trick employees into revealing their login credentials, financial information, or other sensitive data, or into clicking on malicious links that install malware.

Ransomware attacks pose another significant threat to law firms. In these attacks, malicious software encrypts a law firm's data, rendering it inaccessible until a ransom is paid to the cybercriminals. Even after paying the ransom, there is no guarantee that the data will be successfully recovered, and these attacks can cause significant operational disruptions and financial losses.

Law firms are also vulnerable to various types of malware infections, including viruses, spyware, and Trojans. These malicious software programs can infiltrate a law firm's systems without the users' knowledge, allowing attackers to steal sensitive data, monitor activities, or gain unauthorized access to the network.

Threats can also originate from within the law firm itself. Insider threats, whether intentional or unintentional, can lead to data breaches. Intentional insider threats may involve employees deliberately stealing or misusing sensitive information, while unintentional threats can occur through negligence, such as falling victim to phishing scams or mishandling confidential data.

Cybercriminals frequently exploit software vulnerabilities in outdated or unpatched systems to gain unauthorized access to law firm networks. Regularly updating software and applying security patches is crucial to address these known vulnerabilities and prevent exploitation.

The use of weak passwords and the failure to implement multi-factor authentication (MFA) also represent significant vulnerabilities for law firms. Easily guessable or reused passwords can be readily compromised by attackers, and the absence of MFA means that even if a password is stolen, an additional layer of security is lacking.

Finally, poor document management workflows and inadequate security for devices such as printers and mobile phones can create entry points for cyberattacks. Leaving sensitive documents unsecured, failing to properly dispose of old records, or using unsecured personal devices for work purposes can all expose confidential client information.

B. Types of Sensitive Client Information at Risk

Law firms handle a vast array of sensitive client information that is highly attractive to cybercriminals. This includes Personally Identifiable Information (PII) such as names, addresses, social security numbers, driver's license numbers, and tax identification numbers. The compromise of PII can lead to identity theft and other significant harms for affected individuals.

Law firms also frequently possess Personal Health Information (PHI) from clients, including patient names, addresses, medical records, voice data, and video deposition transcripts. As discussed earlier, PHI is subject to strict regulations under HIPAA, and its breach can result in significant legal and financial consequences for both the law firm and its clients.

Financial information, such as credit card numbers and bank account details, is another highly sensitive category of data held by some law firms. This type of information is particularly valuable to cybercriminals for perpetrating financial fraud.

Uniquely critical to the legal profession is the vast amount of confidential attorney-client communications and privileged information that law firms maintain. This can include case details, legal strategies, intellectual property, trade secrets, and information related to mergers and acquisitions. The compromise of this type of information can have severe legal and business ramifications for clients, potentially impacting ongoing litigation, business transactions, and competitive advantage.

3: RESPONDING TO A DATA BREACH: A STEP-BY-STEP GUIDE

A. Immediate Actions Upon Discovery of a Breach

The initial moments after discovering a potential data breach are critical for mitigating its impact. Recognizing the signs of a data breach is the first crucial step. These signs can include unusual network activity, such as large amounts of data being transferred at odd hours, system failures or crashes, the appearance of unfamiliar files or programs, or the receipt of ransom demands. Once a potential breach is suspected, the law firm should immediately activate its incident response plan, if one exists. A well-defined and regularly tested incident response plan provides a structured framework for a coordinated and effective response.

The next immediate action should be to secure the affected systems and prevent further unauthorized access, a process known as containment. This may involve isolating compromised computers or network segments, changing passwords, and temporarily shutting down affected services. Simultaneously, the firm should initiate a preliminary assessment to determine the scope and nature of the breach. This initial assessment aims to understand what happened, what types of data may have been affected, and how the breach might have occurred, providing a foundation for the subsequent steps in the response process.

B. Notification Requirements

Following the discovery and initial assessment of a data breach, law firms face crucial notification obligations to both their clients and regulatory bodies.

1. Clients: Under Rule 1.4 of the New York Rules of Professional Conduct, lawyers have an ethical duty to promptly inform current clients of a cybersecurity incident that constitutes a material development in the representation. This ethical imperative necessitates transparent communication with affected clients, providing them with sufficient information about the nature of the breach, the specific types of their information that may have been involved, the steps the law firm has taken to address the incident, and any potential mitigation measures the client should consider taking to protect themselves. While there is no explicit ethical rule requiring notification to former clients, law firms should consider potential legal obligations, particularly if personally identifiable information was compromised, and may choose to notify former clients as a matter of professionalism.

2. Regulatory Bodies (SHIELD Act): The New York SHIELD Act mandates notification to several state agencies in the event of a data breach affecting the private information of New York residents. These agencies include the New York State Attorney General (NYAG), the New York Department of State (DOS), and the New York State Police. A critical recent amendment to the law, effective December 21, 2024, imposes a strict 30-day deadline for notifying affected individuals after the discovery of the breach. Furthermore, law firms that are considered covered entities under the regulations of the New York Department of Financial Services (NYDFS) have an additional requirement to notify NYDFS of the breach. The notification to these state agencies must include specific information about the timing, content, and distribution of the notices sent to affected individuals, as well as the approximate number of individuals impacted and a copy of the consumer notice template. In cases where a data breach affects more than 5,000 New York residents, the law firm is also required to notify major consumer reporting agencies.

3. Regulatory Bodies (HIPAA): For law firms acting as business associates under HIPAA, a distinct notification obligation exists. The business associate must notify the covered entity of a breach of unsecured PHI without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. This notification allows the covered entity to fulfill its own HIPAA obligations, which include notifying the affected individuals, the Department of Health and Human Services (HHS), and, in breaches affecting over 500 individuals, potentially the media.

C. Conducting a Thorough Investigation and Remediation

A critical component of responding to a data breach is conducting a thorough investigation to understand the incident and implement appropriate remediation measures. Law firms should consider engaging cybersecurity experts and legal counsel to assist with this process. Cybersecurity experts can help identify the source and method of the breach, assess the extent of the data compromise (determining which specific data was accessed or exfiltrated), and implement corrective actions to secure the affected systems and prevent future occurrences. Legal counsel can provide guidance on navigating the complex legal and regulatory landscape, ensuring compliance with notification requirements and advising on potential legal liabilities.

The investigation should aim to pinpoint how the breach occurred, what vulnerabilities were exploited, and what specific data was accessed or taken. This understanding is crucial for implementing effective remediation measures to eradicate the threat and restore the security and integrity of the law firm's systems. Throughout the entire incident response process, it is essential to meticulously document the incident, the steps taken to respond, and the findings of the investigation. This documentation is vital for legal and compliance purposes, as well as for informing future security improvements.

4: PREVENTION AND MITIGATION: BUILDING A ROBUST SECURITY POSTURE

A. Implementing Reasonable Administrative, Technical, And Physical Safeguards (As Required By The Shield Act)

The New York SHIELD Act mandates the implementation of reasonable administrative, technical, and physical safeguards to protect the private information of New York residents.

1. Administrative Safeguards focus on the management and oversight of the data security program. These include designating one or more employees to coordinate the security program; identifying risks in network and software design;

assessing risks in information processing, transmission, and storage; detecting, preventing, and responding to attacks or system failures; regularly testing and monitoring the effectiveness of key controls, systems, and procedures; protecting against unauthorized access to or use of private information; and disposing of private information securely. A critical technical safeguard is data encryption, both when data is stored (at rest) and when it is being transmitted (in transit).

2. Physical Safeguards are designed to protect the physical access to sensitive data. These include assessing risks of information storage and disposal; detecting, preventing, and responding to intrusions; and protecting against unauthorized access to or use of private information during or after collection, transportation, and destruction or disposal. Secure disposal of physical records containing private information is also essential.

B. Best Practices for Law Firm Cybersecurity

Beyond the specific requirements of the SHIELD Act, implementing broader cybersecurity best practices is crucial for law firms to effectively protect client data and meet their ethical obligations. Comprehensive employee training and awareness programs are paramount, providing regular and mandatory training on topics such as identifying phishing emails, creating and maintaining strong passwords, and proper data handling procedures. Implementing strong password policies and utilizing password management tools can significantly reduce the risk of unauthorized access.

Utilizing data encryption for all sensitive client information, both when it is stored and when it is transmitted, provides a critical layer of defense. Conducting regular security audits and risk assessments, both internally and by engaging external experts, helps identify vulnerabilities and ensure the effectiveness of security measures. Implementing multi-factor authentication (MFA) for all logins adds an essential layer of security by requiring users to provide more than just a password. Securing wireless networks and remote access through the use of Virtual Private Networks (VPNs) is crucial, especially with the increasing prevalence of remote work. Regularly updating and patching all software and operating systems is vital to address known security vulnerabilities. Implementing strict access controls and adhering to the principle of least privilege ensures that employees only have access to the data necessary for their specific roles. Developing and maintaining a comprehensive Written Information Security Plan (WISP) documents the firm's security policies and procedures. Implementing data loss prevention (DLP) measures can help prevent sensitive information from leaving the firm's control. Finally, ensuring the secure disposal of old hardware and media is essential to prevent unauthorized access to residual data.

C. Developing and Implementing an Effective Incident Response Plan

A crucial component of a robust security posture is having a well-defined and regularly tested incident response plan. This plan should outline the steps to be taken in the event of a cybersecurity incident or data breach. Key elements of an effective incident response plan include creating a dedicated incident response team with clearly defined roles and responsibilities; establishing clear communication protocols, both internally within the firm and externally with clients and regulatory bodies; defining incident severity levels and establishing specific response procedures for each level; outlining the step-by-step process for incident identification, containment, eradication, recovery, and post-incident review (to identify lessons learned); and, critically, regularly testing and updating the plan through methods such as tabletop exercises that simulate real-world cyberattack scenarios.

- **Summary of Key Legal Provisions:**
  - Excerpts and summaries of the New York SHIELD Act, focusing on the definitions of private information and a data breach, the requirements for reasonable safeguards, and the notification obligations.
  - Key requirements of HIPAA for business associates, including the definition of PHI, the obligations under the Privacy, Security, and Breach Notification Rules, and the requirements for Business Associate Agreements.
  - Summaries of New York Rules of Professional Conduct Part 1200, specifically Rules 1.1 (Competence), 1.4 (Communication), 1.6 (Confidentiality of Information), 1.15 (Preserving Identity of Funds and Property of Others), and 5.1, 5.2, and 5.3 (Responsibilities of Law Firms, Partners, Managers, Supervisory Lawyers, and Nonlegal Assistants).

- **Data Breach Response Checklist:**
  - A checklist outlining immediate steps upon discovery (e.g., activate incident response plan, contain the breach), notification procedures (clients, NYAG, DOS, State Police, NYDFS if applicable, consumer reporting agencies, covered entity under HIPAA), investigation steps (engage experts, identify source and scope), and remediation efforts (secure systems, implement corrective actions, document the incident).
- **Cybersecurity Best Practices Guide for Law Firms:**
  - A guide summarizing administrative safeguards (e.g., security awareness training, risk assessments), technical safeguards (e.g., firewalls, intrusion detection, data encryption), and physical safeguards (e.g., access controls, secure disposal). Includes tips on password management, MFA, securing remote access, and regular software updates.
- **Links to Relevant Statutes and Ethical Opinions:**
  - Link to the full text of the New York SHIELD Act: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
  - Link to relevant sections of HIPAA regulations: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html and https://www.hhs.gov/hipaa/for-professionals/security/index.html
  - Link to the New York Rules of Professional Conduct Part 1200: https://www.nysba.org/attorney-resources/professional-standards/

- Links to cited NYSBA and NYC Bar ethics opinions (e.g., Opinion 842, Formal Opinion 2024-3) available on their respective websites.

Requirement	**New York SHIELD Act**	**HIPAA (for Business Associates)**
Who to Notify	Affected New York residents, NYAG, NY Department of State, NY State Police, NYDFS (for regulated entities), Consumer Reporting Agencies (if > 5,000 residents affected)	Covered Entity
Notification Timeline	Individuals: Within 30 days of discovery; State Agencies: Most expedient time possible, without delaying notice to residents	Covered Entity: Without unreasonable delay, no later than 60 days after discovery
Key Information to Include	Description of the breach, type of data affected, steps individuals can take, contact information, details of notification to state agencies	Nature of the breach, identification of affected individuals (if possible), type of PHI involved, date of breach and discovery, actions taken to mitigate harm
Trigger for Notification	Unauthorized access to or acquisition of private information that compromises confidentiality, security, or integrity	Breach of unsecured PHI

Category of Safeguard	**Specific Safeguard**	**Description/Explanation**	**Relevant Legal/Ethical Requirement**
Administrative	Employee Training	Regular, mandatory training on cybersecurity awareness, including phishing, password security, and data handling.	SHIELD Act Administrative Safeguard; NY RPC Rules 1.1, 1.6, 5.1, 5.3
Administrative	Risk Assessments	Periodic assessments to identify internal and external security risks and evaluate the effectiveness of existing safeguards.	SHIELD Act Administrative Safeguard; NY RPC Rules 1.1, 1.6, 5.1, 5.3
Technical	Data Encryption	Encrypting sensitive client information both at rest and in transit.	SHIELD Act Technical Safeguard; NY RPC Rule 1.6
Technical	Multi-Factor Authentication (MFA)	Requiring users to provide two or more verification factors for all logins.	Cybersecurity Best Practice; NY RPC Rule 1.6
Technical	Software Updates and Patching	Regularly updating and patching all software and operating systems to address known vulnerabilities.	Cybersecurity Best Practice; SHIELD Act Technical Safeguard
Physical	Access Controls	Implementing measures to limit physical access to areas where sensitive data is stored.	SHIELD Act Physical Safeguard; NY RPC Rule 1.6
Physical	Secure Disposal	Establishing and following secure procedures for the disposal of both electronic and physical records containing private information.	SHIELD Act Physical Safeguard; NY RPC Rule 1.6, 1.15

Conclusion

Data security is not merely an IT concern but a fundamental aspect of a New York lawyer's ethical and legal obligations. The increasing sophistication and frequency of cyberattacks targeting law firms necessitate a proactive and ongoing commitment to protecting client information. Lawyers must understand the legal framework established by the New York SHIELD Act and, where applicable, HIPAA, as well as the ethical duties outlined in the New York Rules of Professional Conduct and relevant ethical opinions. By implementing reasonable administrative, technical, and physical safeguards, developing and regularly testing a comprehensive incident response plan, and fostering a culture of security awareness within their firms, New York lawyers can significantly minimize the risk of data breaches and ensure they are prepared to respond effectively if an incident does occur. A proactive approach to cybersecurity is not only essential for compliance with legal and ethical requirements but also for maintaining client trust and the integrity of the legal profession in the digital age. Resources such as the New York State Bar Association and the New York City Bar Association offer valuable guidance and support to assist lawyers in navigating this complex and critical area.

Sources

1. Top Law Firm Data Breaches and Cyberattacks - imageOne, https://www.imageoneway.com/blog/law-firm-data-breaches

2. 10+ Law Firm Cybersecurity Best Practices - NordLayer, https://nordlayer.com/blog/law-firm-cybersecurity-best-practices/

3. Inside the Breach: Real-Life Tales of Law Firm Hacks and Data Leaks - Threat Intelligence, https://www.threatintelligence.com/blog/law-firm-data-breach

4. Data breaches in the legal industry: Is your information safe? - One Legal, https://www.onelegal.com/blog/data-breaches-in-the-legal-industry/

5. Why Law Firm Data Breaches Are Skyrocketing in 2024 | ProcessBolt, https://processbolt.com/insights/blog/why-law-firm-data-breaches-are-skyrocketing-in-2024/

6. Cybersecurity for Law Firms: Protecting Client Data in a Digital World ., https://www.aaepa.com/2025/03/cybersecurity-for-law-firms-protecting-client-data-in-a-digital-world/

7. Research Reveals Data Breaches On The Rise at UK Law Firms | Tripwire, https://www.tripwire.com/state-of-security/research-reveals-data-breaches-rise-uk-law-firms

8. Wolf Haldenstein Confirms 3.4 Million-record Data Breach - The HIPAA Journal, https://www.hipaajournal.com/wolf-haldenstein-data-breach/

9. Biggest law firm cyber attacks and trends - Embroker, https://www.embroker.com/blog/law-firm-cyber-attacks/

10. Top Law Firm Data Breach Examples From 2023 - ChartRequest, https://chartrequest.com/law-firm-data-breaches-2023/

11. N.Y. Comp. Codes R. & Regs. Tit. 22 § 1200.1.6 ... - Law.Cornell.Edu, https://www.law.cornell.edu/regulations/new-york/22-NYCRR-1200.1.6

12. Confidentiality of information, N.Y. Comp. Codes R. & Regs. tit. 22 § 1200.1.6, https://casetext.com/regulation/new-york-codes-rules-and-regulations/title-22-judiciary/subtitle-b-courts/chapter-iv-supreme-court/subchapter-e-all-departments/part-1200-rules-of-professional-conduct/subpart-client-lawyer-relationship/section-120016-confidentiality-of-information

13. selected sections of the New York Rules Of Professional Conduct (eff. 4/1/09), http://nassau18b.org/forms/5.Selected_Rules_of_Conduct.pdf

14. Interesting Provisions in New Rules: Rule 1.6(b) through Rule 1.7, https://www.newyorklegalethics.com/interesting-provisions-in-the-new-rules-rule-1-6b-through-rule-1-7/
15. Rule 1.6: Confidentiality of Information - American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/
16. proposed amendment to rule of professional conduct 1.6 – authorizing disclosure of confidential information of - New York City Bar Association, https://www.nycbar.org/pdf/report/uploads/20071914-ProposedAmendmenttoRuleofProfessionalConduct1.6.pdf
17. New York Bar Issues Ethics Opinion on Protecting "Confidential" Client Identity Information on Smartphones - Hunton Andrews Kurth LLP, https://www.hunton.com/privacy-and-information-security-law/new-york-bar-issues-ethics-opinion-on-protecting-confidential-client-identity-information-on-smartphones
18. Ethics Opinion 842 - New York State Bar Association, https://nysba.org/ethics-opinion-842/
19. Formal Opinion 2017-5: An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information* | New York City Bar Association, https://www.nycbar.org/reports/formal-opinion-2017-5-an-attorney%EF%BF%BD%EF%BF%BD%EF%BF%BDs-ethical-duties-regarding-u-s-border-searches-of-electronic-devices-containing-clients%EF%BF%BD%EF%BF%BD%EF%BF%BD-confidential-informatio/
20. Cybersecurity Concerns For Lawyers: Practical And Ethical Considerations Roadmap - New York State School Boards Association, https://www.nyssba.org/clientuploads/nyssba_pdf/Events/nysasa-cybersecurity-ethics-webinar-02082023/02_slides-rev2.pdf
21. Ethics Opinion 1019 - New York State Bar Association, https://nysba.org/ethics-opinion-1019/
22. Ethics Opinion 1020 - New York State Bar Association, https://nysba.org/ethics-opinion-1020/
23. https://www.law.cornell.edu/regulations/new-york/22-NYCRR-1200.1.1
24. Rule 1.1: Competence - American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/

25. New_York_Rules_of_Professional, https://sps.columbia.edu/sites/default/files/2021-11/new_york_rules_of_professional_conduct_rules_1.1_and_4.1.docx

26. 11 RULE 1.1: COMPETENCE (a) A lawyer should provide competent representation to a client. Competent representation requires the - University at Buffalo Law School, https://www.law.buffalo.edu/content/dam/law/content/cle/200612-materials-2.pdf

27. Ethical eDiscovery for New York Lawyers | Trustpoint.One, https://trustpoint.one/ethical-ediscovery-for-new-york-lawyers/

28. Rule 1.1 Competence - Comment - American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/

29. NYSBA Proposed Rules of Professional Conduct — Part III | New York Legal Ethics Reporter, https://www.newyorklegalethics.com/nysba-proposed-rules-of-professional-conduct-part-iii/

30. part 1200 - Rules Of Professional Conduct - UC Berkeley Law, https://www.law.berkeley.edu/wp-content/uploads/2015/04/ny-rules-prof-conduct-1.11.pdf

31. Feature Article: Competence in a Changing Profession - Joseph, Hollander & Craft LLC, https://josephhollander.com/news-blog/competence-in-a-changing-profession/

32. Ensuring Security: Protecting Your Law Firm and Client Data - American Bar Association, https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2024/ensuring-security-protecting-your-law-firm-and-client-data/

33. Law Firm Data Security: Ethics and Risk Mitigation - Clio, https://www.clio.com/resources/cybersecurity/ethics-and-risk-mitigation/

34. The Ubiquitous Threat of a Data Breach Your Ethical Duties to Mitigate the Risks, https://www.cccba.org/article/the-ubiquitous-threat-of-a-data-breach-your-ethical-duties-to-mitigate-the-risks/

35. SHIELD Act | New York State Attorney General, https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

36. Stop Hacks and Improve Electronic Data Security Act ("Shield Act") NY State Senate Bill S5575 New York Rules of Professional, https://www.nycourts.gov/LegacyPDFS/accesstojusticecommission/tc/2023/2A-Agents-of-SHIELD-CLE-Resources.pdf

37. New York Shield Act - PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/new-york-shield-act.html

38. Shield Act - domecile, https://www.domecile.com/about/shield_act

39. NY Shield Act Data Sheet 9-9-20_vFinal.indd - PCA Technology Group, https://www.pcatg.com/wp-content/uploads/PCA-NY-SHIELD-Act-Datasheet.pdf

40. The NY SHIELD Act [A Compliance Checklist] - Just Solutions, Inc, https://www.justinc.com/blog/the-ny-shield-act-compliance-checklist/

41. The New York SHIELD Act - Spirion, https://www.spirion.com/solutions/compliance/new-york-shield-act

42. NY SHIELD Act: What It Is and How to Make Sure Your Business Complies - CMIT Solutions, https://cmitsolutions.com/rochester-ny-1109/blog/what-is-the-ny-shield-act/

43. What the New York SHIELD Act Means for Your Business - TermsFeed, https://www.termsfeed.com/blog/ny-shield-act/

44. New York SHIELD Act: Everything You Need to Know for Compliance - Centraleyes, https://www.centraleyes.com/new-york-shield-act/

45. Understanding the New York SHIELD Act - Usercentrics, https://usercentrics.com/knowledge-hub/new-york-shield-act/

46. Understanding New York's Updated Data Breach Notification Law - HR Works, https://hrworks-inc.com/industry-update/understanding-new-yorks-updated-data-breach-notification-law/

47. New York | Summary of U.S. State Data Breach Notification Statutes | Davis Wright Tremaine, https://www.dwt.com/gcp/states/new-york

48. New York Data Breach Law Amended: New Timelines and Expanded Regulatory Reporting, https://www.thompsonhine.com/insights/new-york-data-breach-law-amended-new-timelines-and-expanded-regulatory-reporting/

49. New York Amends its Data Breach Notification Law | Byte Back, https://www.bytebacklaw.com/2025/02/new-york-amends-its-data-breach-notification-law/

50. New York Adopts Amendment to the State Data Breach Notification Law | Inside Privacy, https://www.insideprivacy.com/cybersecurity-2/new-york-adopts-amendment-to-the-state-data-breach-notification-law/

51. New Year, New Data Breach Notification Requirements in New York: Impactful Changes for Life Sciences and Consumer Health Care Companies |

Insights, https://www.ropesgray.com/en/insights/alerts/2025/01/new-year-new-data-breach-notification-requirements-in-new-york

52. A MoFo Privacy Minute: New York Data Breach Notification | Morrison Foerster, https://www.mofo.com/resources/insights/250314-a-mofo-privacy-minute-new-york-data-breach-notification

53. HIPAA Privacy & Security | New York Healthcare Lawyers Health Law Partners, https://www.thehealthlawpartners.com/hipaa-privacy-security.html

54. HIPAA Compliance Lawyers - Wachler & Associates, P.C., https://www.wachler.com/practice-areas/hipaa-compliance-lawyers/

55. HIPAA Privacy Rules for the Protection of Health and Mental Health Information - New York State Office of Mental Health, https://omh.ny.gov/omhweb/hipaa/phi_protection.html

56. HIPAA Compliance - Law Offices of Pullano & Farrow, https://www.lawpf.com/hipaa-compliance

57. HIPAA Requirements for Attorneys - Atlantic.Net, https://www.atlantic.net/hipaa-compliant-hosting/hipaa-requirements-for-attorneys/

58. www.bakerdonelson.com, https://www.bakerdonelson.com/files/Uploads/Documents/TheHIPAApotamusintheRoom.pdf

59. HIPAA and Healthcare Privacy | Practices - Holland & Knight, https://www.hklaw.com/en/services/practices/healthcare/hipaa-and-healthcare-privacy

60. Law Firm HIPAA Compliance: What You Need to Know, https://compliancy-group.com/law-firm-hipaa-compliance/

61. What Law Firms Should Know About HIPAA Compliance | U.S. Legal Support - JDSupra, https://www.jdsupra.com/legalnews/what-law-firms-should-know-about-hipaa-6636032/

62. HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules - CMS, https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf

63. HIPAA Breach Notification Rule | American Medical Association, https://www.ama-assn.org/practice-management/hipaa/hipaa-breach-notification-rule

64. Complying with FTC's Health Breach Notification Rule | Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0

65. HIPAA Breach Notifications – A Question of Timing | Alerts and Articles | Insights, https://www.ballardspahr.com/insights/alerts-and-articles/2024/01/hipaa-breach-notifications-a-question-of-timing

66. HIPAA Regulations: Notification in the Case of Breach -- Notification By Business Associates - § 164.410 - Bricker Graydon LLP, https://www.brickergraydon.com/insights/resources/key/hipaa-regulations-notification-in-the-case-of-breach-notification-by-business-associates-164-410

67. Formal Opinion 2024-3: Ethical Obligations Relating to a Cybersecurity Incident - NYC Bar Association, https://www.nycbar.org/reports/formal-opinion-2024-3-ethical-obligations-relating-to-a-cybersecurity-incident/

68. When Should Law Firms Notify Clients About Data Breaches? - American Bar Association, https://www.americanbar.org/groups/business_law/resources/business-law-today/2020-november/when-should-law-firms-notify-clients/

69. Ethics Opinion 1268: Confidential information; publication of article about issues arising in a case handled by the lawyer - New York State Bar Association, https://nysba.org/ethics-opinion-1268-confidential-information/

70. Ethics Opinion 1249 - New York State Bar Association, https://nysba.org/ethics-opinion-1249/

71. A Guide to Law Firm Cybersecurity Risks & Ethical Compliance - Enzoic, https://www.enzoic.com/blog/law-firm-cybersecurity/

72. Holding Funds and Property Under RPC 1.15, https://www.cgpllp.com/assets/uploads/pdf/Holding_Funds_and_Property_Under_RPC1.15.pdf

73. N.Y. Comp. Codes R. & Regs. tit. 22 § 1200.1.15 | https://casetext.com/regulation/new-york-codes-rules-and-regulations/title-22-judiciary/subtitle-b-courts/chapter-iv-supreme-court/subchapter-e-all-departments/part-1200-rules-of-professional-conduct/subpart-client-lawyer-relationship/section-1200115-preserving-identity-of-funds-and-property-of-others-fiduciary-responsibility-commingling-and-misappropriation-of-client-funds-or-property-maintenance-of-bank-accounts-record-keeping-examination-of-records

74. Rule 1.15: Safekeeping Property - American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property/

75. N.Y. Comp. Codes R. & Regs. Tit. 22 § 1200.1.15 ... - Law.Cornell.Edu, https://www.law.cornell.edu/regulations/new-york/22-NYCRR-1200.1.15

76. Rule 1.15 - Law Ledgers, https://www.lawledgers.com/rule-1-15/

77. The Top 5 Cybersecurity Risks for Law Firms | Uptime Practice™, https://uptimepractice.com/cybersecurity-risks-for-law-firms/

78. Cybersecurity for Lawfirms | Common Threats & Solutions - Darktrace, https://darktrace.com/cyber-ai-glossary/cybersecurity-for-law-firms

79. A guide to data security for law firms - Embroker, https://www.embroker.com/blog/cybersecurity-for-law-firms/

80. Small Law Firms and Their Data Are Extremely Vulnerable to Cyberattacks - Bitdefender, https://www.bitdefender.com/en-us/blog/hotforsecurity/small-law-firms-and-their-data-are-extremely-vulnerable-to-cyberattacks

81. Security Awareness Training for Legal Professionals - Keepnet Labs, https://keepnetlabs.com/blog/security-awareness-training-for-legal-professionals

82. Cybersecurity Awareness for Law Firm Employees - State Bar of Wisconsin, https://www.wisbar.org/NewsPublications/WisconsinLawyer/WisconsinLawyerPDFs/98/02/41_43.pdf

83. Security Awareness Training for Law Firms - TeachPrivacy, https://teachprivacy.com/security-awareness-training-for-law-firms/

84. Cyber Security Awareness Training for Law Firm Industry - CybeReady, https://cybeready.com/lawfirm-security-awareness-training

85. Cybersecurity for Law Firms | Uptime Practice™, https://uptimepractice.com/cybersecurity-for-law-firms/

86. A Guide to Cybersecurity Compliance for Law Firms - The National Trial Lawyers, https://thenationaltriallawyers.org/article/cybersecurity-compliance-guide/

87. Tabletop Exercises: Real Life Scenarios and Best Practices - Threat Intelligence, https://www.threatintelligence.com/blog/cyber-tabletop-exercise-example-scenarios

88. Cybersecurity: Law Firm Data Breach come in Different Forms - PracticePanther, https://www.practicepanther.com/blog/cybersecurity-data-breach-types/

89. The Law Firm Guide to Cybersecurity - Washington State Bar Association, https://www.wsba.org/for-legal-professionals/member-support/practice-management-assistance/guides/cybersecurity-guide

90. Law Firm Guide to Cybersecurity - American Bar Association, https://www.americanbar.org/groups/law_practice/resources/tech-report/archive/law-firm-guide-cybersecurity/

91. 11 Best Cybersecurity Practices to Protect Your Firm - Joseph F. Rice School of Law, https://sc.edu/study/colleges_schools/law/about/news/2020/11_best_cybersecurity_practices.php

92. How To Pass A Cyber Security Audit for Law Firms - Cirrus Technology Services, https://cirrusts.com/how-to-pass-a-cyber-security-audit-law-firms/

93. What Lawyers Need to Know About Law Firm Data Encryption - Embroker, https://www.embroker.com/blog/law-firm-data-encryption/

94. Cybersecurity for Law Firms | Ensure Your Business's Security - Sygnia, https://www.sygnia.co/solutions/law-firms/

95. New Developments in Law Firms' Obligations to Protect Against Data Breaches - New York Law Journal, https://www.moundcotton.com/news-updates/new-developments-in-law-firms-obligations-to-protect-against-data-breaches/

96. KEY TAKEAWAYS - New York State Bar Association, https://nysba.org/app/uploads/2022/01/NYSBA-Cyber-3rd-TL-Report-FINAL-012022.pdf

97. SHIELD Act: Compliance Guide for New York Employers, https://mosey.com/blog/new-york-shield-act/

98. Incident Response Planning A Musthave For Law Firms | - SecureTrust Cybersecurity, https://securetrust.io/blog/incident-response-planning-a-musthave-for-law-firms/

99. 10 Best Practices for Incident Response Plans [2024] - Daily.dev, https://daily.dev/blog/10-best-practices-for-incident-response-plans-2024

100. A Two-Pronged Approach to Cyber Security and Incident Response Planning | American Bar Association, https://www.americanbar.org/content/dam/aba/publications/professional_lawyer/24-3/preventiand-response-twopronged-approach-cyber-security-and-incident-response-planning.pdf

101. Incident Response: Best Practices for Quick Resolution | Atlassian, https://www.atlassian.com/incident-management/incident-response

102. Law Firm Data Encryption: Guide to Legal Professional - MatterSuite, https://www.mattersuite.com/law-firm-data-encryption/

103. Data Encryption Essentials for Law Firms - CaseFox, https://www.casefox.com/blog/law-firm-data-encryption/

104. Implementing Effective Data Encryption Strategies In Legal Practices |, https://securetrust.io/blog/implementing-effective-data-encryption-strategies-in-legal-practices/

105. A primer on data encryption best practices for law firms - Logikcull, https://www.logikcull.com/blog/primer-data-encryption-best-practices-law-firms

106. 8 Strategies to Ensure Cybersecurity for Law Firms - Rev, https://www.rev.com/blog/cybersecurity-for-law-firms

107. IT Security Audit for Law Firms: Going Over the Basics - 365 IT Services, https://365itservices.ca/it-security-audit-for-law-firms/

108. Law Firm Internal Audits | Corporate Investigation Consulting, https://corporateinvestigation.com/law-firm-consulting/internal-audits/

INCIDENT RESPONSE PLAN FOR DEWEY CHEATUM & HOWE LAW FIRM

OUTLINE

- **Introduction:** Purpose of the incident response plan, its scope (systems, data, offices covered), and objectives. Note the sensitive data handled (PHI, PII, client confidences, financial info) and the need to protect it. Reference compliance requirements (NY SHIELD Act, HIPAA, NY Rules of Professional Conduct, NYSBA cybersecurity guidance) that mandate having such a plan (nysba.org).
  - *Purpose:* Define the plan's goal to provide a clear framework for responding to security incidents, minimizing damage, and meeting legal/ethical obligations.
  - *Scope:* State that it applies to all staff, IT systems, and data (client files, communications, databases, etc.) at the firm's New York offices. Include third-party services and cloud storage as applicable.
  - *Objectives:* Ensure rapid detection, containment of threats, protection of client data, compliance with notification laws, preservation of evidence, timely recovery, and lessons learned.
- **Roles and Responsibilities:** Define an Incident Response Team (IRT) and key roles. Include internal team members and any external resources. Clearly outline each role's duties during an incident (e.g. Incident Coordinator, IT Support, Managing Partner, Compliance Officer, etc.). Provide contact information for each role. A table may be used to list roles,

assigned personnel, and their contact details for quick reference. Ensure one or more employees are designated to coordinate security and response (a NY SHIELD Act requirement (ag.ny.gov). Also note responsibilities of *all employees* (e.g. reporting incidents promptly).

- **Incident Definition and Classification:** Define what constitutes a “security incident” or “data breach” for the firm (e.g. unauthorized access to client data, malware infection, lost device with firm data, ransomware, etc.). Classify incidents by severity/impact levels (e.g. Low, Medium, High) to gauge response urgency. A table of severity levels with definitions and examples can be included (for example, *High* = confirmed compromise of client PII/PHI or major system outage; *Medium* = limited data exposure or single system malware; *Low* = attempted intrusion blocked by firewall, etc.). This helps determine escalation and notification requirements for each level.
- **Incident Detection and Reporting:** Describe how incidents are detected and how staff should report them. Include both technical detection (firewall/antivirus alerts, suspicious logins via 2FA, system logs) and user reporting (staff noticing unusual computer behavior, discovering a lost laptop or mis-sent email, etc.). Outline the immediate steps upon suspicion of an incident: who to contact (e.g. notify the Incident Response Coordinator or IT support *immediately*, via a 24/7 contact number/email). Provide an incident report form or checklist for gathering key details (date, time, type of incident,

systems involved). Emphasize a culture of prompt reporting without fear of blame, so that issues are brought forward quickly.

- **Containment and Mitigation:** Steps to limit the incident's damage once identified. This section details how to isolate affected systems (e.g. disconnect a compromised computer from the network, disable a breached user account, block malicious IPs at the firewall). If malware (like ransomware) is spreading, instruct to quarantine infected machines and *not* power them off (to preserve memory evidence) unless instructed. For data breaches, secure any exposed information (e.g. change credentials, revoke access). Include guidance on preserving evidence during containment (for example, imaging affected drives or collecting logs before wiping malware) for later analysis. If needed, the plan should advise contacting external IT specialists or forensics at this stage to assist in containment. List any containment resources (backup servers, spare laptops, etc.).
- **Eradication and System Recovery:** Once contained, outline how to eliminate the threat (remove malware, fix vulnerabilities) and then restore systems to normal operation. Steps might include running antivirus scans, applying security patches, resetting compromised passwords firm-wide (especially if an account was hacked), and verifying that backups are free of malware before restore. For example, if a server was compromised, rebuild or clean the server and then restore data from backups. Ensure data integrity and that no "backdoors" or malicious accounts remain. This section also

covers data recovery procedures: how to recover lost or encrypted data from backups, and how to rebuild any damaged databases or files. Clearly state where backups are stored and who is responsible for data restoration. Before full restoration, test the systems in a safe environment to confirm the threat is eradicated. Document all remedial actions taken.

- **Notification and Communication:** Detail the communication plan during and after an incident. This includes:
  - *Internal Escalation:* Who within the firm must be informed and when (e.g. managing partners must be informed of High-severity incidents within X hours; all staff should be alerted if they need to take action like changing passwords).
  - *Client Notification:* When and how to inform clients whose information was compromised. The firm's ethical duty under NY State professional rules requires notifying clients of breaches affecting their confidential data. Specify that the Relationship Partner or a designated attorney will promptly inform affected clients about the nature and scope of the breach and steps being taken, in plain language, while maintaining attorney-client privilege as appropriate.
  - *Regulatory Notifications:* Outline required notifications to authorities:
    - **NY SHIELD Act:** If "private information" (e.g. SSNs, driver's license numbers, credit card or account numbers with security codes, biometric data, etc.) was accessed by an unauthorized

party, the firm must notify the affected New York residents "in the most expedient time possible"ag.ny.gov. The firm must also notify New York state regulators. New York law requires notice to the Attorney General's office, State Police, and Department of State regarding the breach and notices sent ag.ny.gov. The plan should state that the firm will submit the **NYAG Data Breach Reporting** form (online portal) to satisfy regulator notice, which automatically notifies the necessary state agencies and credit reporting agencies. Include a reference to the notification statute for clarityag.ny.gov. If the breach affects over 5000 NY residents, mention that consumer credit agencies must also be notified (though the AG's portal covers this).

- **HIPAA:** If the incident involves Protected Health Information (PHI) (e.g. files from healthcare clients), the firm (as a Business Associate) must follow HIPAA breach notification rules. The plan should require performing a HIPAA risk assessment (to determine if PHI was compromised and the probability of compromise) and **notify the covered entity** client without unreasonable delay and no later than 60 days from discovering the breach. The notification to the healthcare client should include identification of each individual affected and details of the breach, so the client can fulfill their obligation to notify patients and HHS. (If the law firm is itself a covered entity for any reason, it would directly notify affected individuals, HHS, and possibly media for breaches over 500 individuals hhs.gov hhs.gov, but in most cases the firm will be acting as a Business Associate to clients.) The plan must ensure coordination with the client's privacy officer on breach response.

    - **Other Regulations:** If data of individuals from other states is involved, the firm will comply with those states' breach laws as applicable (each state has its own notification requirements). If applicable, also comply with federal regulations (like Gramm-Leach-Bliley for financial data, if the firm handles certain financial client records). However, focus remains on NY and HIPAA as primary frameworks.

- *Law Enforcement:* If a crime is suspected (e.g. hacking, ransomware, theft of data), consider notifying law enforcement. The plan should state criteria for involving law enforcement such as the FBI Cyber Crime unit or local police. Typically, for ransomware or serious breaches, reaching out to law enforcement and the FBI Internet Crime Complaint Center (IC3) is recommended once initial containment is done. Coordinate this with counsel – maintaining client confidentiality is crucial, so only reveal necessary information. Note any required delays if law enforcement asks the firm to delay notifying clients or public (NY law permits delay if law enforcement determines notification would impede an investigation (ag.ny.gov).

  - *Communication Plan:* Designate a spokesperson (e.g. a senior partner or communications director) for any external communications (press or public statements) to ensure consistent messaging. In a small firm, this might be the managing partner. Emphasize that no employee should communicate about the incident externally except through approved channels. If media notice is required (for example, a HIPAA-covered client breach affecting 500+ people, or if the breach becomes public), prepare a press release in coordination with the client and counsel. Maintain attorney-client privilege in communications by involving legal counsel in drafting notifications. The plan might include template notification letters for clients and regulators as appendices.

- **Incident Documentation and Investigation:** Throughout the incident, maintain a detailed incident log. Document all facts, actions, and decisions (time of discovery, people involved, containment steps, eradication steps, communications, etc.). This is important for internal review and required for some regulations (e.g. documentation is part of NY SHIELD's "security program" record-keeping). Also, ensure evidence is collected and preserved: log files, copies of affected data, forensic disk images if needed. The plan should instruct that any forensic analysis (e.g. determining the cause, which data was accessed, and the extent of damage) be carried out or guided by qualified experts. If outside forensic investigators are engaged, ideally have outside breach counsel retain them to preserve legal privilege. Ensure chain-of-custody for evidence if there's potential for legal proceedings.

- **Recovery and Restoration:** After eradication, bring systems back online safely. Verify that all systems are patched and secured before reconnecting to the production network. Restore data from backups as needed and verify the integrity of restored data. This section should include testing of systems post-recovery (for example, verify that a cleaned system is no longer communicating with malicious hosts, run vulnerability scans to confirm the threat is gone). If operations were disrupted (e.g. email or billing system down), execute the business continuity procedures to resume work (perhaps the firm has a continuity plan to operate manually or via alternate systems temporarily). Also, if any data was permanently lost, determine if that data can be reconstructed or if its loss needs to be communicated (for instance, lost client records). Communicate internally when it’s safe to resume normal use of systems or if any passwords need to be changed firm-wide (commonly done after a breach).
- **Post-Incident Review and Lessons Learned:** Once the incident is resolved, convene a post-incident meeting with the Incident Response Team and relevant staff/partners. This should happen ideally within a week of resolution (while fresh). Review what happened, how well the response went,

and identify any gaps or delays. Document lessons learned and recommendations. For example, if the breach occurred due to a missing patch or an insecure practice, plan how to remediate that (upgrade software, enhance firewall rules, provide additional staff training, etc.). Evaluate if notification processes and communications went smoothly or if improvements are needed. This section should also assign follow-up tasks: updating this incident response plan if necessary, revising policies, or conducting additional training. **Update the incident response plan** to incorporate lessons (the NY SHIELD Act expects adjustment of the security program in light of new circumstances (ag.ny.gov). Also, consider if additional security measures are needed (maybe implementing an Intrusion Detection System, contracting a 24/7 monitoring service, enabling logging that was missing, etc., based on the incident). If not already in place, the firm might decide to obtain or update cyber insurance coverage as part of remediation.

- Additionally, ensure **reporting** to any oversight committees or firm leadership. Senior management or the partnership should receive a summary of the incident and remediation actions. This demonstrates accountability and helps justify any budget increases for security.
- **Training and awareness:** If the incident revealed user mistakes (e.g. someone fell for a phishing email), plan a refresher training for all staff on security awareness. Regular drills can be mentioned here: e.g. *"The firm will conduct an annual incident response tabletop exercise"* to

practice this plan so that employees and the IRT stay familiar with their roles. This helps fulfill the "training employees in security program practices" requirement of NY SHIELDag.ny.gov and maintains readiness.

- **Plan Maintenance:** State who is responsible for maintaining and updating this IR plan (e.g. the Incident Response Coordinator or Compliance Officer). The plan should be reviewed at least annually and after any significant incident. Updates should reflect changes in personnel, IT infrastructure, client regulatory requirements, or laws. Record version numbers and dates of revision. Also, keep a **secure copy** of the plan accessible even if the network is down (for example, a printed copy in the office and an offline file accessible to the IRT). Make sure all attorneys and staff know how to access the plan and are briefed on their roles.

DETAILED INCIDENT RESPONSE PLAN FOR DEWEY CHEATUM & HOWE LAW FIRM

1. Introduction

Purpose: This Incident Response Plan establishes a structured approach for responding to cybersecurity and data breach incidents at **Dewey Cheatum & Howe Law Firm**. The firm specializes in corporate transactions, real estate, healthcare, trusts & estates, and commercial litigation, and it handles highly sensitive information (including Protected Health Information (PHI), Personally Identifiable Information (PII) such as Social Security numbers, driver's license and financial account details, confidential client communications, and other sensitive financial data like credit card numbers and EINs). The purpose of this plan is to enable the firm to respond swiftly and effectively to any security incident, minimizing damage and exposure, protecting client confidentiality, and ensuring compliance with all applicable laws and ethical duties. It outlines the steps to identify, contain, eradicate, and recover from incidents, and to communicate appropriately with clients, authorities, and stakeholders.

Scope: This plan applies to all **personnel (attorneys and staff)** of Dewey Cheatum & Howe Law Firm and all **information systems** and data repositories used in the firm's operations. It covers incidents affecting the firm's office networks, computers, mobile devices, cloud services, and any third-party systems under the firm's control. Both cybersecurity incidents (e.g. malware attacks, network intrusions, ransomware, data theft) and other data breaches (such as lost/stolen devices or inadvertent disclosures of client information) are within scope. The plan is designed for the firm's New York operations and client data, and takes into account New York State laws and regulations. It should be followed in conjunction with the firm's other policies (e.g. confidentiality policy, acceptable use policy). If an incident involves systems or data outside this scope, the principles here can still guide the response, but additional procedures may be needed.

Objectives: Key objectives of the incident response plan include: *(1)* **Rapid detection** of incidents and immediate notification of the incident response team; *(2)* **Containment** of threats to prevent further damage or unauthorized access; *(3)* **Protection of client data and confidentiality**, honoring our ethical obligations as attorneys; *(4)* **Compliance** with all legal and regulatory notification requirements (such as the NY SHIELD Act and HIPAA breach rules) in a timely manner; *(5)* **Eradication** of the root cause of the incident (such as removing malware or closing security vulnerabilities); *(6)* **Recovery** of IT systems and data to resume normal operations as quickly and safely as possible; and *(7)* **Post-incident analysis** to learn from the event and improve our security posture going forward. Meeting these objectives will help limit financial loss, reputational damage, and legal penalties that could result from incidents.

Compliance Framework: This incident response plan is built to ensure adherence to important **legal and ethical requirements**:

NY SHIELD Act (N.Y. Gen Bus Law §899-bb): Requires businesses that handle private information of New York residents to maintain reasonable safeguards (administrative, technical, physical) to protect that data, and to include incident detection and response measures. It also mandates prompt notification to affected individuals and the NY Attorney General's office (and other state agencies) in the event of a data breach involving private information. This plan incorporates those requirements, including designating individuals to coordinate security efforts and outlining breach notification procedures.

- **HIPAA (Health Insurance Portability and Accountability Act):** As the firm handles PHI on behalf of healthcare clients (making the firm a *Business Associate* under HIPAA), we must comply with the HIPAA Security Rule and Breach Notification Rule. The Security Rule requires policies for addressing security incidents (45 C.F.R. §164.308(a)(6)), and the Breach Notification Rule requires that breaches of unsecured PHI are reported to the covered entity without unreasonable delay and no later than 60 days from discovery. This plan ensures any incident involving PHI triggers the required risk assessment and notification to our client (the covered entity) with details and a list of affected individuals, so that the client can fulfill patient and regulator notifications within HIPAA's timelines. (A failure to comply with HIPAA can also be deemed a violation of the SHIELD Act, underscoring the importance of diligence.)
- **New York State Rules of Professional Conduct:** As lawyers, we have a fundamental ethical duty to safeguard client confidentiality.

Rule 1.6(c) in New York requires that **“A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, [confidential client information]”**. This plan is a key part of our effort to fulfill that duty by providing a mechanism to respond if confidentiality is compromised. Additionally, ethics opinions (e.g. NYSBA Op. 842) indicate that if a lawyer discovers a breach of client data (even through a third-party like a cloud storage provider), the lawyer **must investigate and notify any clients affected**. Therefore, our plan includes prompt client notification as an essential step when client information is at risk, in line with our professional responsibilities.

- **NYSBA Guidelines:** The New York State Bar Association recommends that law firms implement robust cybersecurity practices, including having a formal incident response plan with written steps for investigating, responding to, and reporting cyber incidents. This document follows those best practices (as well as industry-standard frameworks like NIST) to ensure our approach is comprehensive and aligns with bar association guidance.
- **Other Applicable Laws:** The plan also keeps in mind other data protection laws that may apply to specific cases (for example, state breach laws for non-NY residents, or client-specific regulations like FTC safeguards if dealing with consumer finance data). The

overarching principle is to **comply with the most stringent applicable requirements**. In case of any conflict between laws, the firm's legal counsel will determine the appropriate course, but generally this plan is designed to meet all overlapping obligations.

2. Roles and Responsibilities

Effective incident response requires clear definition of roles. Dewey Cheatum & Howe Law Firm designates the following roles as part of its **Incident Response Team (IRT)**:

Role	Assigned To	Responsibilities
Incident Response Coordinator (Incident Manager)	*Designated IT Manager or Security Officer* (e.g. John Doe, IT Director)	**Lead coordinator** for any incident. Initiates the incident response plan when an incident is reported. Assesses initial incident information, classifies the incident's severity, and activates other team members as needed. Ensures all steps of response are carried out and documented. Serves as primary point-of-contact for internal reporting. Also responsible for managing the security program overall, as required by NY SHIELD.
IT Support/Technical Lead	*IT Specialist or External IT Provider*	Works under the Coordinator to investigate technical aspects. Analyzes alerts, contains affected systems (e.g. disconnects devices, applies firewall blocks), removes malware, and restores systems from backup. Provides technical evidence (logs, forensic images) to support investigation. If the firm lacks in-house IT, coordinates with external IT consultants or a

Role	Assigned To	Responsibilities
		managed service provider fulfilling this role.
Compliance & Privacy Officer (Legal Compliance Lead)	*Attorney in charge of compliance (e.g. Jane Smith, Partner)*	Focuses on regulatory and legal compliance during incident. Determines what notification requirements are triggered (NY SHIELD, HIPAA, etc.) and ensures they are fulfilled on time. Coordinates with clients on breach notifications, especially for PHI breaches (serving as liaison to the client's privacy officer). Keeps abreast of the New York State breach laws and ethical duties. Drafts or reviews notification letters to regulators and clients. May also coordinate with outside counsel if specialized breach counsel is engaged.
Managing Partner/Executive	*Managing Partner or designated senior partner*	Makes high-level decisions, such as approving public communication, deciding whether to pay a ransom (if ransomware occurs) or shut down certain systems. Communicates with other partners about the incident's business impact. Authorizes engagement of external parties (forensic firm, outside counsel, etc.) and resource allocation (e.g. funds for emergency IT purchases). Also may act as the spokesperson for press or public statements if needed. Ensures that client service continuity (e.g. court deadlines) is managed during the disruption.
Communications Coordinator (could be	*Firm's Communications*	Handles outward communications. Drafts internal alerts to staff and talking points. If client notifications

Role	Assigned To	Responsibilities
same as Managing Partner or a PR lead)	*Director or appointed attorney*	or public statements are needed, ensures they are clear and accurate (with input from legal/compliance). Manages any media inquiries. If the firm has cyber insurance, this role may also be responsible for notifying the insurer and coordinating any resources they provide.
Outside Experts (as needed)	*External Cybersecurity Consultant, Forensic Investigator, or Breach Coach Attorney*	The firm may retain external specialists in a serious incident. For example, a digital forensics team to determine the extent of a network breach, or an outside **breach coach** (cybersecurity attorney) to help navigate complex legal obligations and preserve attorney-client privilege These experts report to the Incident Response Coordinator and Managing Partner. The plan should be flexible to integrate their advice. (Contact information for pre-vetted vendors is maintained separately.)
All Employees (General Staff)	*All attorneys and support staff*	**First line of detection and defense.** Employees must follow security best practices to prevent incidents (per training and firm policies). Crucially, they must **report any suspected incident immediately** to the Incident Response Coordinator or a supervisor. This includes lost devices, strange computer behavior, suspected phishing emails, or knowledge of a possible confidentiality breach. Employees should assist the IRT as needed (for example, providing information

Role	Assigned To	Responsibilities
		about what they observed, cooperating with containment steps such as shutting down a PC if instructed). Staff are expected to maintain confidentiality about the incident (not to spread news to those without a need-to-know or externally) to protect the firm and clients during the response.

Assignment of Personnel: The table above lists roles and their responsibilities. The firm should assign specific people to each role (and a backup if possible). For instance, *John Doe* (IT Manager) might be the Incident Coordinator, with *Jane Smith* (Partner) as backup coordinator if John is unavailable. A current contact list with 24/7 phone numbers for all team members is maintained in Appendix A of this plan (not included here, but to be filled in by the firm). The roles may overlap for a small firm – e.g., one person might wear multiple hats – but the responsibilities still need to be covered. All team members must be familiar with this plan and their duties under it.

Authority: The Incident Response Coordinator has the authority to take necessary steps to mitigate an incident, including ordering a temporary shutdown of systems to contain damage, if delay to get approval would exacerbate the situation. Major decisions (like engaging law enforcement, paying ransom, widespread client notification) should be made in consultation with the Managing Partner and Compliance Officer. The plan should be formally approved by firm leadership, giving the IRT the mandate to act decisively when incidents occur.

3. Incident Definition and Classification

Not every security event is a full-blown incident. This section defines what we consider an **"incident"** and how we gauge its severity:

- **Security Incident Definition:** For purposes of this plan, an *incident* is any event that **jeopardizes the confidentiality, integrity, or availability** of the firm's information or information systems. This includes confirmed **breaches of sensitive data** (client or employee information), **cyberattacks** causing disruption or unauthorized access, and **suspected** incidents that could reasonably result in data loss or damage if not addressed. Examples of incidents:
    - A malware infection (virus, ransomware) on a firm computer or server.
    - Unauthorized access to a system or email account (e.g. hacker or insider accessing data without permission).
    - A lost or stolen laptop, smartphone, or portable drive that contained unencrypted client information.
    - Accidental disclosure of confidential data (such as an email with client PII sent to the wrong recipient outside the firm).
    - Detection of significant attempts to breach the network (e.g. firewall logs showing a successful intrusion or an internal system connecting to a known malicious IP).

  - A third-party vendor used by the firm (e.g. cloud document storage or an e-discovery platform) notifying us that they experienced a breach that could affect our data.
  - **Physical security incidents** that may lead to data exposure (like an office break-in where computers or files are stolen).

  The plan should be invoked for any of the above situations. If there is uncertainty whether an event qualifies, staff should err on the side of reporting it so that the Incident Response Coordinator can evaluate the risk.

- **Incident Classification (Severity Levels):** To organize response efforts, the Incident Response Coordinator will classify each incident into one of the following categories, based on scope and impact:
  - **High Severity (Level 3)**
    - Major incident with **significant impact or high risk** to sensitive data or operations. Examples: Large-scale ransomware attack encrypting critical servers; confirmed theft of clients' confidential data (PII/PHI) by an attacker; any breach that triggers legal notification to dozens or hundreds of individuals; prolonged network outage affecting the whole firm; or an incident likely to cause substantial financial or reputational harm.
    - **Response:** All hands on deck. Immediately activate the full Incident Response Team. Notify senior management at once.

Likely requires external assistance (forensics, law enforcement) and formal breach notifications to clients and authorities.

- **Medium Severity (Level 2)**
    - Moderate incident, localized or with limited damage, but still affecting sensitive information or business operations to some extent. Examples: Malware infection on one user's computer that accessed a few client files; a single client's records mistakenly emailed to an incorrect party; a brief outage of email or database with moderate disruption; lost device that is encrypted (reducing risk) but still reportable.
    - **Response:** Incident Response Coordinator and necessary team members handle it. Contain and remediate quickly, possibly with limited outside help. May or may not require client notification or regulatory reporting depending on whether protected data was actually exposed. Keep management informed.
- **Low Severity (Level 1)**
    - Minor security events or incidents with **minimal impact** and no indication of sensitive data compromise. Examples: An isolated virus that was caught and quarantined by antivirus with no damage; an employee's spam email clicked but no

infection occurred; minor policy violations or attempted attacks that were thwarted (e.g. firewall blocked an intrusion attempt).

    - **Response:** Primarily IT handles cleanup. Still document the incident and investigate to confirm it's fully resolved, but broader team activation may not be needed. Use it as a training moment if appropriate. Generally no external notifications required, though internal awareness might be raised (e.g. remind staff of phishing risks).

These severity levels help determine the urgency and the extent of escalation. The Coordinator will assign a provisional severity as soon as enough info is available, and adjust if needed as the investigation unfolds. The plan's actions are scalable: a low-severity issue might just require a simple fix and brief report, whereas a high-severity incident will trigger all sections of this plan in detail.

- **Recording Classification:** The incident record (see Documentation section) should note the severity level and rationale. This could be important later for regulatory documentation or insurance reports. For example, New York's SHIELD Act expects organizations to keep records of any data incidents even if notice wasn't required (and why not required), so classifying an event as low severity/non-breach with reasoning (e.g. "data was encrypted, or attack failed") will support that.

4. <u>Incident Detection and Reporting</u>

Rapid detection is crucial. DCH relies on both technical controls and vigilant personnel to detect potential incidents:

- **<u>Monitoring and Detection Systems</u>:** The firm has in place security tools such as **firewalls**, **antivirus/anti-malware software**, and **two-factor authentication (2FA)** logs for remote access. These systems provide alerts on suspicious activities. For example, the firewall may alert if there are repeated unauthorized login attempts or if it blocks traffic flagged as malicious. Antivirus on endpoints will notify if it quarantines malware. The 2FA system might alert if an unusual login (e.g. from an unrecognized device or location) is attempted on an email or cloud account. Additionally, any intrusion detection or email security systems in use should be tuned to warn of anomalies (like numerous emails to external addresses containing large attachments, which could indicate data exfiltration). IT staff or the managed service provider should regularly review security logs from these systems. While continuous real-time monitoring might not be available 24/7 in a small firm, designated IT personnel should at least have daily checks of logs and an email/SMS alert system for critical events (for example, a firewall could send an email alert if it detects a possible breach). The Incident Response Coordinator is responsible for ensuring these detection capabilities are operational and for investigating any alerts they generate.

- **<u>Employee Awareness</u>:** Often, employees are the ones who notice signs of trouble. All staff are trained to recognize and report potential security incidents. Such signs include: unusual pop-up messages or ransomware notes on their computer, files that suddenly won't open (possible encryption), an lost or stolen work laptop/phone, encountering client data in a location it shouldn't be, or receiving emails from colleagues that seem suspicious (which might mean the colleague's email was hacked). The firm's training (per the NY SHIELD Act's mandate to train employees on security practices emphasizes reporting *anything odd* – "if you see something, say something." This open reporting culture helps catch incidents early.
- **<u>Reporting Procedure</u>:** When an employee suspects an incident, they must **immediately** report it to the Incident Response Coordinator (or alternate contact if Coordinator is unavailable). Multiple reporting channels are provided: a dedicated **Incident Hotline number** (office and cell numbers) and a special email address (e.g. *security@xyzlaw.com*) that forwards to the IRT. The plan should list these contacts clearly (e.g. *"Report incidents to John Doe, IT Director, at 555-1234 (cell 24/7) or 555-5678 (office), or email security@xyzlaw.com"*). For critical incidents out of hours, calling by phone is encouraged to wake the on-call person. If the employee cannot reach the Coordinator, they should escalate to any member of the Incident Response Team or a supervisor. **Time is of the essence** – even a delay of a few hours

can worsen a breach – so the policy is to report first, and then stay available to help.

Upon receiving a report, the Incident Response Coordinator will log the time and initial information and begin the initial assessment (see next section). The employee who reported (or discovered the issue) should not feel obligated to fix or investigate it themselves – in fact, they are advised *not* to tinker with the system (to avoid altering evidence or letting the problem worsen) beyond the minimum necessary to stop immediate damage (like unplugging a network cable if something extreme is happening). Their job is to report and then follow instructions from the IRT.

- **Incident Intake Form:** The Incident Response Coordinator (or whomever first responds) should use an **Incident Report Form** to gather information. This form (sample in Appendix B) will include: date and time of detection, who/what reported it, description of what was observed, systems or data involved (if known), and any immediate actions taken. For example, if a staff member clicked a phishing link, the form would note what link, what machine they were on, and if any credentials were entered. If a device is lost, note when/where it was lost and whether it was encrypted. This structured intake ensures no key detail is overlooked in the heat of the moment. All team members should know where to find this form (both in hardcopy and on the network share) and how to fill it.

- **<u>Initial Analysis and Verification</u>:** The Incident Response Coordinator (with IT support) will quickly analyze the report to verify if it is indeed a security incident and not a false alarm or benign event. This might involve checking the affected system's status, running a quick malware scan, or viewing log entries. For example, if an intrusion alert came from the firewall, the IT lead might correlate it with server logs to see if any connection was actually established. If an employee reports "my files are encrypted and there's a ransom note on screen," that's clearly an incident (ransomware) and verification is straightforward. But if someone reports "I clicked a weird email," IT might check that user's PC for malware traces to confirm if an infection happened. **False positives** (like an AV alert that turned out to be a harmless file) should also be documented but labeled as no incident. However, until confirmed otherwise, the team treats the situation as an active incident.
- **<u>Engaging the IRT</u>:** Based on the initial findings, the Coordinator will classify the incident severity (as per Section 3) and activate the Incident Response Team members appropriate for that level. For high severity, likely the whole team (IT, Compliance, Managing Partner, etc.) is notified immediately (e.g. via a group text or call tree: Coordinator calls Managing Partner and IT support; Managing Partner alerts other partners, etc.). For a medium incident, maybe just IT and Compliance leads are engaged initially. The Coordinator should explicitly communicate to the team: what happened,

what is suspected, and initial steps underway. This can be done in a quick conference call or a team chat channel set up for incidents. Getting everyone on the same page early prevents confusion and ensures tasks aren't overlooked.

5. Containment and Mitigation

Once an incident is confirmed, **containing the threat** is the top priority. The goal of containment is to limit the scope of the incident and prevent further damage or data loss. The specific containment strategy will depend on the nature of the incident, but general guidelines include:

- **Isolate Affected Systems:** Quickly disconnect or isolate the systems known or believed to be compromised. For instance, if a PC is infected with ransomware or malware, **remove it from the network** (unplug Ethernet cable, turn off Wi-Fi). If an email account is suspected of being hacked, **disable the account or change its password** to lock out the attacker. In a network-wide attack, it might be necessary to take certain servers offline or block certain network segments. Speed is crucial – containment actions often need to be done within minutes of confirming an active breach. The firm's IT support will use available tools (remote management, firewall console, etc.) to quarantine systems.
- **Stop Data Exfiltration:** If the incident involves data being actively stolen (exfiltrated) or an intruder in the system, containment may involve blocking the attacker's access. For example, add firewall rules to block outgoing traffic

to the attacker's IP addresses, or turn off the compromised server's network connection. If a specific user's credentials are compromised, **lock that account** and any other accounts the attacker might be using.

- **Apply Temporary Fixes:** Sometimes containment means applying a quick patch or workaround. For instance, if a zero-day exploit is being used and a known workaround exists (like disabling a certain service), do that immediately firm-wide. Or if a web server is under attack via a certain port, temporarily disable that service until a fix can be implemented.
- **Preserve Evidence During Containment:** While containment is critical, we must also **preserve forensic evidence** for later analysis and for satisfying legal requirements. The team should take care not to destroy data that could help understand the incident. For example, instead of wiping an infected computer right away, first isolate it, then make a forensic image of its disk or memory if possible. If logs indicate suspicious activity, back up those log files before they roll over or get lost. The plan might instruct: *"For any system that's taken offline, do not power it down unless necessary – isolate network instead – since memory forensics might be useful. If you must shut it off or it's a personal device, document that fact."* The Incident Response Coordinator should ensure someone (perhaps an external forensic specialist if engaged) is assigned to evidence preservation. Chain-of-custody procedures may be initiated for any evidence that could end up in court or regulatory investigations.

- **<u>Communication During Containment</u>:** The IRT should keep internal communication open as containment actions are taken. A designated person (often the Coordinator or IT Lead) should be updating the team: e.g. "Server X has been taken offline," "We have reset the compromised email passwords," etc. This helps everyone understand the current status. If containment requires informing the broader staff (for example, telling everyone *"Please disconnect from VPN now"* or *"Stop using email until further notice"* to contain an email breach), the Communications Coordinator or Managing Partner will send out an urgent firm-wide alert with instructions.
- **<u>Short-Term Workarounds</u>:** Containment might disrupt normal operations (e.g., if a file server is shut down to stop a breach). The team should implement short-term workarounds to allow business continuity where possible. For example, if the file server is offline, perhaps use a clean backup server or temporary cloud storage for urgent client documents (but only if secure to do so). If email is down, use phones or alternate means to communicate with clients briefly. These decisions should be guided by the Managing Partner balancing client service with security needs.
- **<u>External Containment Help</u>:** If the situation is beyond internal capabilities (e.g., a widespread network compromise or a sophisticated malware), the Coordinator should quickly consider bringing in outside experts. Pre-identified contacts (like a cybersecurity firm on retainer via insurance, or a trusted IT consultant) can assist remotely to contain the

threat. For example, they might deploy an endpoint threat detection tool across all machines to identify and isolate infected ones. The plan should note any such contracts or retainer agreements and how to trigger them (e.g. notify the cyber insurance hotline for immediate incident response assistance).

- **Examples of Containment Actions:** To illustrate, here are a few scenario-specific steps:
  - *Malware/Ransomware on one PC:* Remove network cable, inform user not to use the PC. IT will then run a scan in safe mode or image the drive. Check if network drives were impacted; if so, disconnect those drives.
  - *Server breach (web or database server hacked):* Take the server offline from the internet (disable its switch port or AWS instance, etc.). Change admin passwords that were used on it. Check other servers for the same indicators (maybe contain them too if they show signs).
  - *Email account compromise:* Lock account, review email audit logs to see if attacker set up forwarding rules or downloaded mail. Remove any malicious rules, and possibly recall any rogue emails sent from the account if feasible.
  - *Lost laptop:* If it had remote wipe capability (e.g., via a mobile device management tool), trigger a wipe as soon as it is online. Change any

passwords that were saved on it. Publicize internally if someone finds a rogue device connecting.

  - *Data leakage by mis-sent email:* If an email with PII was sent to the wrong person, attempt to contact the recipient asking deletion/confidentiality. This is more mitigation than containment, but it's an immediate action to reduce further spread of data.

- **Ensure Safety Before Moving On:** Only once the immediate threat is contained (the "bleeding has stopped") should the team move into the next phases of full eradication and recovery. Containment may be short (minutes/hours) or extended (days) depending on incident complexity. In some cases, you might implement **"two-stage" containment**: a quick initial isolation, then a more considered longer-term containment strategy. For example, in a ransomware outbreak, initial containment is disconnecting everything; longer-term containment might be bringing systems up one by one in a segmented network to safely clean them.

The result of this phase is that the incident is at least temporarily halted – the virus is no longer spreading, the intruder's access is cut off, or the leaked data is no longer actively being taken. Now the firm can catch its breath a bit and proceed to eradication and investigation with less urgency than the initial scramble.

6. Eradication and System Recovery

After containing the incident, the firm must **eliminate the threat completely** and restore systems to normal, secure operation. This phase involves thorough investigation, root cause removal, and careful recovery of data and functionality:

- **<u>Root Cause Analysis</u>:** The IT Lead (often with help from forensic experts) will investigate how the incident happened and what the scope was. This means determining the **attack vector** (phishing email? unpatched software? stolen password?) and identifying all systems or data that were affected. For example, if malware was detected, what kind is it? Did it spread elsewhere? If a server was breached, what vulnerability did they exploit and what did they do on the server? This analysis guides eradication, you must know what you're removing. All relevant logs, alerts, and evidence collected during containment are reviewed in detail now. If needed, conduct interviews (e.g., ask the user what exactly they did when they noticed the issue, etc.). In complex cases, an external forensic investigation might be warranted to ensure no stone is unturned. The team should document the findings, as this will also feed into notification content (clients/regulators will want to know what happened and that it's fixed).
- **<u>Eradication of Threat</u>:** Based on the above analysis, take actions to remove the attacker or malware from all affected areas:
  - For malware infections: remove malicious software from systems by running updated antivirus/anti-malware tools on all potentially affected machines. Sometimes, manual removal or re-imaging the machine is safer. Ensure that any **malicious files or processes** are

eliminated. If the malware created backdoor user accounts or scheduled tasks, delete those. In ransomware cases, use clean backups rather than paying ransom if possible (paying is discouraged due to ethical and legal considerations, plus no guarantee of success; involve law enforcement and only consider payment as a last resort with management approval).

- For hacking/intrusion: close the vulnerabilities they used. For instance, if an attacker got in through an unpatched software flaw, apply the patch or temporarily disable that service. If they stole credentials, **change all passwords** that might have been compromised (not just the one account; assume they might have grabbed others). This may mean firm-wide password reset for certain systems if scope is uncertain. Also, check for any **tools or malware the attacker left** (like sniffers, web shells, or user accounts). Remove or neutralize them. This step can be quite involved; a forensic scan of systems should be done to search for known indicators of compromise.
- For data breaches: if data was stolen or exposed, you obviously cannot "un-steal" it from the attacker, but eradication in this context means ensuring the path of leakage is closed. E.g., if data was being exfiltrated through an open port or misconfigured database, fix that configuration. If a rogue employee was copying data, terminate their access. So, cut off any ongoing access to sensitive data.

  - For each affected system, **rebuild or clean** it to a trustworthy state. Sometimes the only safe way is to wipe the system and reinstall from scratch (especially critical servers) because you cannot be 100% sure a sophisticated attacker hasn't left hidden backdoors. The plan should specify that for high-severity compromises, a clean rebuild is preferred over trying to meticulously clean a live system, unless time constraints demand otherwise.
- **<u>Verification</u>:** After performing eradication steps, **verify that systems are clean and secure**. This might involve:
  - Running multiple scanning tools (antivirus, anti-rootkit, etc.) to ensure no malware remains.
  - Checking system integrity (files, registry, configurations) against known good baselines if available.
  - Ensuring that any compromised accounts are secured and no unauthorized access persists (reviewing user lists, group memberships, login logs post-change).
  - If applicable, having a third-party do a penetration test or vulnerability scan after fixes to confirm the holes are indeed patched.
  - Monitoring the network closely for a period of time for any signs that the threat is still present or trying to return. For example, if we blocked an IP during containment, watch if there are more attempts from other IPs.

- **System Restoration:** Once confident that the threat is eradicated, begin **bringing systems back online** in a controlled manner. Prioritize critical systems first (e.g., restore file servers, practice management software, email). Steps include:
    - **Recovering data from backups:** If data was corrupted or encrypted, retrieve the most recent clean backup. The firm should maintain regular encrypted backups of key systems (daily, offsite if possible). Now those backups will be used to restore functionality. Follow the restore procedure carefully and verify completeness. For instance, if a database was wiped by the attacker, restore the last nightly backup and then check that all recent transactions are present (or identify what's missing to possibly re-enter).
    - **System rebuilds:** For compromised machines, either re-image them (format and reinstall OS) or replace them with new hardware if necessary. Then apply all updates/patches before restoring data. Hardening steps should be taken (disable unnecessary services, install improved security tools if we identified a need).
    - **Configuration changes:** Implement improved security configurations to prevent recurrence. For example, if an intrusion happened because remote desktop was open on a server, after rebuild ensure remote desktop is turned off or restricted to VPN. If a user fell for phishing,

consider implementing an email filtering rule or 2FA for that service (the firm already uses 2FA, but maybe enforce it more broadly).

  - **Gradual reconnect:** Don't connect everything at once blindly. Perhaps bring up one segment at a time and test. For example, reconnect a cleaned server to the network and watch its behavior. Then allow users to connect. Maintain heightened logging during this period in case something was missed.

- **Data Integrity and Validation:** After restoration, it's vital to confirm that recovered data is intact and correct. Randomly sample some documents, emails, or database records to ensure they are the expected versions and not corrupted. If any data is found missing or irrecoverable, decide on next steps (maybe notify the affected client if it's their data, or see if there's another source for that data). For instance, if some days of emails are lost, inform the users to reconstruct important communications as needed.
- **Coordination with Users:** As systems come back, communicate to staff which systems are now available and any precautions they must take. Often after a breach, all users may be required to **change their passwords** on restored systems (especially if there's a chance credentials were compromised). Provide guidance on creating strong new passwords or set up the system to force a reset on next login. If multi-factor authentication was not already enforced on a system involved in the breach, now is the time to implement it – e.g., require token codes for remote email access forthwith.

- **Incremental Approach:** If the incident was severe, consider not resuming full operations until certain that critical pieces are secure. In some cases, the firm might operate in a limited mode (only most essential IT services up) for a day or two while continuing verification, rather than rushing everything online and risking a reinfection. The Incident Response Coordinator in conjunction with the Managing Partner will decide when to declare "all clear" and normal IT operations restored.
- **Documenting the Eradication and Recovery:** Throughout this phase, log every action: which systems were rebuilt, which backups were used (include backup dates/times), any issues encountered during restore, etc. This log will be invaluable for the post-incident review and for any auditors or regulators who later question how we handled things. For example, HIPAA requires documentation of breaches and response, and having a clear record shows diligence.

By the end of this phase, the firm's systems should be clean, data restored, and business operations largely back to normal (or perhaps with some temporary workarounds still, but functional). Importantly, the vulnerabilities that led to the incident have been addressed, so the same attack should not reoccur.

7. Notification and Communication Procedures

Communicating appropriately is a critical part of incident response – both to meet legal requirements and to maintain trust with our clients and stakeholders. This section describes **who needs to be notified, when, and how** in the event of a confirmed data breach or other significant incident, as well as general internal and external communication protocols.

- **<u>Internal Notifications and Escalation</u>:** Internally, the Incident Response Team will keep the firm's leadership and relevant personnel informed. For high-severity incidents, the entire partnership should be briefed as soon as practical (in an emergency meeting or conference call) by the Managing Partner or Incident Coordinator. This briefing includes what happened, what is being done, and what the potential impacts are (especially any impacts on clients or case deadlines). For incidents that may affect the day-to-day work of employees (e.g., email server down, or instructions to not use certain systems), the Communications Coordinator will send firm-wide emails or texts with clear instructions. For example, *"Our file system is under maintenance due to an IT issue; please do not attempt to access drive X until further notice. IT will update when available."* Keeping employees in the loop helps prevent rumors and ensures cooperation with any mitigation steps (like everyone needing to change passwords).
- **<u>Client Notification (Confidentiality Breach)</u>:** If an incident results in, or is reasonably suspected to have resulted in, unauthorized access to or disclosure of **client confidential information**, the firm has an ethical obligation to inform those clients. Even if not required by data breach statutes (for example, if the data wasn't PII but was sensitive case information), **client notification is required by our professional duty**.

The plan instructs that the Relationship Partner for each affected client (or another appropriate attorney) will notify the client **promptly** once key facts are known. Typically, after containment and initial investigation, and ideally within a few days of discovery (sooner if the data exposure is confirmed and significant). The notification can be a personal phone call followed by a written communication (letter or secure email) summarizing what occurred and what the firm is doing about it. It should avoid panic, stick to facts, and reassure the client of steps taken. According to ABA and NYSBA guidance, lawyers should tell clients about breaches that **impact their matters or expose their data** so the client can make informed decisions. The content of client notices should include: the general nature of the incident, what client data or files were involved (if known), what the firm has done to contain and remediate, and what is being done to protect the client (for instance, offering credit monitoring if personal data like SSNs were exposed, or simply assuring that documents are being restored). It should also include a person to contact with questions (likely the Relationship Partner or Compliance Officer). All such communications will be coordinated with the Compliance Officer and possibly outside counsel to ensure consistency and to avoid admissions of liability while still being transparent. Timing-wise, we will not unnecessarily delay informing clients, but we may wait until we have accurate information and have contained the issue to avoid providing misleading or incomplete info. (Note: If law enforcement is involved and requests a delay in client notification, we will document that request and comply to the extent permitted, but will ultimately fulfill our ethical duty as soon as allowed.)

- <u>**Regulatory and Legal Notifications**</u>**:**
  - **NY SHIELD Act – Notification to Individuals and State Agencies:** Under New York's data breach law, if a **breach of "private information"** has occurred, the firm must notify affected individuals (New York residents) and certain state agencies. *Private information* under the law includes personal information (name, etc.) plus data elements like Social Security number, driver's license number, financial account or credit card numbers (with security codes), biometric data, or email address with password/security Q&A. It also covers account credentials and, via amendments, perhaps health information if combined with identifiers. If such data was likely acquired by an unauthorized person, we will prepare a **notification letter to the affected individuals**. The law says to notify in the "most expedient time possible and without unreasonable delay" after discovery, consistent with law enforcement needs. Our aim is to send notices within **30 days** if feasible (New York encourages expedient notification; some interpretations suggest within 30 days is a best practice). The letter will include the elements required: a description of the incident in general terms, the types of information compromised, approximate date of breach, what we are doing to handle it, and advice

on what the individual can do (e.g. contact credit bureaus, fraud alerts). We will offer assistance like credit monitoring if SSNs or financial info were exposed (often expected as a good practice).

In addition, we must notify the **Office of the NY Attorney General (OAG)**, the NY Department of State, and the NY State Police. In practice, this is done by submitting the breach details through the OAG's online breach reporting portal. The portal submission will automatically disseminate the info to the other required state contacts and to the nationwide consumer reporting agencies (Equifax, Experian, TransUnion) if the breach affects over 5,000 individuals. The Compliance Officer will be responsible for filing this report, which includes info like timing of breach, number of affected persons, and a copy of the consumer notice letter. We will maintain a copy of all notices and submissions. If the breach affects over 500 NY residents, we understand the Attorney General may follow up or investigate, so our thorough documentation and response will be critical to show we took proper action.

If the firm determines after investigation that an incident **did not actually compromise private information** (for example, a laptop was encrypted and no evidence of access), and thus notification is not legally required, we will document our decision process and evidence supporting it. This documentation will be kept for at least 5 years, as required by law, and if regulators inquire, we can show how we “reasonably determined no harm”.

- **HIPAA Breach Notification – Covered Entities and HHS:** If PHI was compromised and our firm is a **Business Associate**, we are obligated to notify the impacted healthcare Covered Entity client. The HIPAA rule requires the Business Associate to notify the Covered Entity **without unreasonable delay and no later than 60 days** from discovery of the breach. Our goal is to notify much sooner – typically within 10 days of confirming a PHI breach – so that our client can meet their own deadlines (which are also within 60 days to notify patients, and possibly earlier for large breaches to media). The notification to the client will include identification of each individual (patient) whose PHI was affected (or at least the information we have at that time), and any other details the Covered Entity will need for their notification to those individuals and to the Department of Health and Human Services (HHS). We will cooperate fully with the client’s needs, which may include helping to draft the notification to patients or providing a description of the breach and remedial actions. If our client asks us to handle some notifications (HIPAA allows delegation), we will do so as agreed, ensuring the notices meet HIPAA content requirements. In parallel, if the PHI breach is significant (500+ individuals), the Covered Entity will notify HHS and possibly media;

our role is to support them with facts and documentation. We will also likely need to report the incident in our annual security assessment for HIPAA and potentially to the NY AG as it likely overlaps with SHIELD Act if NY patient data (as noted by the Norton Rose analysis, a HIPAA breach often equals a SHIELD Act breach). If the firm itself was a Covered Entity (unlikely except possibly for employee health plan info), then we would directly notify individuals, media (>500) and HHS (<60 days for big breaches, or annually for small breaches) as per 45 C.F.R. §§164.404-408.

- **Other Jurisdictions' Breach Laws:** The Compliance Officer will assess if residents of other states or countries are involved and ensure those legal requirements are met. Most states have laws similar to NY's requiring notice to their residents and sometimes their state attorney general. For efficiency, our notices to individuals will be written in a way to satisfy all applicable jurisdictions (generally if it meets NY's and HIPAA's standards, it will meet others). If any state requires a specific authority to be notified (for instance, some require their Attorney General if a certain number of residents are hit), we will do so. If any international data (like EU personal data) is involved, we will consult with counsel on GDPR or other requirements (e.g. 72-hour notice to supervisory authorities for GDPR if applicable).

- **Law Enforcement Notification:** In cases involving criminal activity – which is most cyber incidents – informing law enforcement can be beneficial and sometimes legally required. The firm will typically contact the **local FBI field office or the FBI's IC3 (Internet Crime Complaint Center)** for significant cybercrimes such as ransomware, major hacks, or theft of identities. The FBI can provide guidance, and reporting may help in any larger investigation of threat actors. We will also consider involving local police, especially if physical theft (like stolen hardware) or if required for insurance claims. The plan notes that New York law does *not* force notifying law enforcement, but does allow us to delay notifying individuals if an official law enforcement letter requests that doing so would impede an investigation. If we receive such a request, we will honor it for the time specified, and diarize to follow up once clearance is given. Any communication with law enforcement will be handled by the Managing Partner or an attorney designee, to ensure privilege and accurate information sharing. We will likely have outside breach counsel coordinate this in significant incidents.
- **Insurance Notification:** If the firm has a **cyber liability insurance policy**, prompt notification to the insurer (or broker) is usually required to invoke coverage. The plan should include contacting our insurance carrier's incident hotline as soon as a notifiable incident is

confirmed (often within 24-48 hours of discovery, depending on policy terms). The Communications Coordinator or Managing Partner will handle this. The insurer may provide resources (like a panel forensic firm or legal counsel) – our plan accounts for integrating those resources as needed, though we maintain the ability to use our chosen vendors if that's allowed. Keeping the insurer in the loop also helps ensure costs (for remediation, notifications, credit monitoring, etc.) are covered per the policy.

  - **Professional Responsibility Disclosure:** Aside from client notification, if the breach significantly impairs our ability to represent clients (e.g., we miss a filing due to systems down, or client data is irretrievably lost), we might have duties to courts or others. While beyond the scope of a pure IR plan, we note to consult ethics counsel if an incident raises such issues.

- **Communication Guidelines:**
  - *Accuracy and Consistency:* All external communications (whether to clients, media, or regulators) will be coordinated to ensure consistency. We will prepare a **written summary** of the incident (as known at that time) to serve as the basis for all notifications, so everyone is on the same page regarding the facts. Any updates will be similarly documented and disseminated to those communicating. This avoids contradictory statements.

- *Privilege Considerations:* Since communication can risk waiving privilege or creating liability, all written communications, especially to clients and public, will be reviewed by legal counsel. We may mark certain investigatory communications as privileged/confidential where appropriate. As recommended, involving counsel in communications (even drafting client notices) can maintain privilege over some aspects of the incident investigation. However, required notifications (like to regulators or individuals) will ultimately become public, so they should be factual and careful in tone.
- *Public Relations:* If the incident becomes public knowledge (for instance, via media or if we choose to issue a press release for transparency, or in the case of a large HIPAA breach which is posted on the HHS public portal), our designated spokesperson (Communications Coordinator or Managing Partner) will handle press inquiries. The firm will prepare a press statement if necessary, focusing on the actions taken and our commitment to security and clients, rather than the specifics of the attack which could invite further exploitation or blame. The message: we responded swiftly, notified those affected, and are preventing future incidents – to maintain trust.
- *Internal Communication:* The plan also covers keeping our own team informed. After the initial containment, periodic status updates should

be given to all firm employees especially if the incident affects their work (like systems downtime or requirement to change passwords). Rumor control is important – staff should hear updates from leadership, not third-party sources. Once the incident is resolved and public/client notifications are done, the Managing Partner or Incident Coordinator will likely hold a short debrief meeting for all staff to explain what happened and reinforce any learnings (without disclosing sensitive details that aren't appropriate to share).

  - *Communication Log:* Maintain a log of all notifications made: dates/times of client calls, copies of letters sent, confirmation of submission to AG portal, etc. This will be part of the incident record and is often needed for compliance verification.

8. **<u>Documentation and Evidence Preservation</u>**

Throughout the incident response process, meticulous **documentation** must be maintained. This serves multiple purposes: forensic investigation, legal compliance, post-incident analysis, and potential future litigation or insurance claims. Key documentation includes:

- **<u>An Incident Timeline</u>**: a chronological record of all events and actions from discovery to recovery. The Incident Response Coordinator (or a scribe assigned) will update this in real-time or retrospectively soon after actions. Each entry should note the date/time, the action or event, and who performed it. For example: "09/15/2025 10:32 – Jane Doe reported ransomware on PC;

10:40 – IT disconnected PC from network; 11:00 – Incident declared Level 3, all IRT members paged," and so on. Time stamps are crucial especially if we later need to demonstrate we notified within required time frames.

- **Technical Findings**: The IT Lead or forensics team should document what they find – malware names, attacker IP addresses, vulnerabilities exploited, accounts compromised, etc. If any malware samples are obtained, note hash values and where stored. If logs are analyzed, highlight the pertinent log entries (with copies saved). This evidence might be shared with law enforcement or used to improve security. If a root cause analysis report is prepared, include that.
- **Communications Record**: As mentioned, keep copies of all formal communications (notification letters/emails to clients, regulators, press releases, internal all-staff memos). If any phone or in-person communications occur (e.g., calling a client to explain), log the date, person spoken to, and summary of what was said. This protects the firm by showing we fulfilled duties and provides a reference if later there's any dispute about who was told what/when.
- **Costs and Hours**: It's wise to track costs incurred and staff time spent (especially for major incidents). This can be useful for insurance claims or ROI calculations for security improvements. For instance, record if we paid for credit monitoring for X clients, or if we had to pay overtime to IT staff, or

an invoice for outside consultants of $Y. This might not be in the heat of the moment but soon after, compile these numbers.

- **Evidence Handling**: Any digital evidence collected (disk images, log files, malware samples) should be stored securely (on an encrypted drive or secured evidence repository). Note who collected it and how (chain-of-custody). If needed, have key evidence notarized or hashed to prove it wasn't altered. This level of rigor is especially important if the incident could lead to legal action (e.g., a client lawsuit or prosecution of an attacker). The plan instructs the team to use forensic tools that make read-only copies and to avoid modifying original data. Physical evidence (like a defective hard drive or printed phishing letter) should likewise be labeled and locked up. We will follow guidance akin to law enforcement evidence handling for any crucial items.

All documentation will be consolidated into an **Incident Report** once things settle. The Incident Response Coordinator, with input from the team, will produce a final report summarizing the incident, actions taken, and results. This report may be reviewed by firm management and legal counsel before finalizing. Non-sensitive portions of it might be shared with clients or regulators if requested or needed to demonstrate compliance.

This documentation not only satisfies regulatory record-keeping (for example, New York's law expects companies to keep breach investigation records, and HIPAA definitely expects documentation of any breach analysis and notifications made), but it also is invaluable for the next section – the lessons learned process.

9. Post-Incident Review and Lessons Learned

After the incident has been handled and operations normalized, Dewey Cheatum & Howe Law Firm will conduct a **post-incident review**. The purpose is to evaluate the response and identify improvements for the future, turning a negative event into an opportunity to strengthen our defenses and response capabilities.

- **Post-Mortem Meeting:** The Incident Response Coordinator will schedule a debrief meeting with the Incident Response Team and any other relevant parties (for example, the staff member who first reported the incident, representatives from departments affected, outside experts who assisted, etc.). This should happen ideally within one to two weeks of the incident resolution. In this meeting, the team will review the incident timeline and report, discussing questions such as:
    - How was the incident detected? Could we have detected it sooner? (Do we need better monitoring or earlier training intervention?)
    - Was our **incident identification and classification** accurate and swift? Did we initially underestimate or overestimate severity?
    - How well did **containment** go? Were there any delays or missteps? (For example, was everyone able to disconnect quickly? Did any containment action cause unexpected side effects?)

  - During **eradication and recovery**, were there tools or knowledge we lacked? Could we have restored faster? Did our backups work as expected (if not, that's critical to fix)?
  - Did we meet all **notification deadlines** comfortably? Were our communications effective (any confusion from clients or regulators)?
  - What went *right*? It's important to note successful aspects of the response to reinforce those practices.
  - What went *wrong* or could be improved? Identify specific gaps: maybe the team realized log collection was insufficient, or a particular software wasn't patched, or staff were unsure who to call at first. Maybe the contact list was outdated (if someone tried to call an old number). All such issues should be noted.
  - Could better **preparation** have prevented the incident altogether? e.g., if the cause was a missed patch or weak password, then clearly an improvement is needed in vulnerability management or password policy.
- **<u>Action Items</u>:** From this discussion, the team will generate a list of concrete action items. Each item should have an owner (person responsible) and a target date. Examples of action items:
  - *Increase cybersecurity training* – e.g. "All staff will undergo a phishing awareness refresher within 30 days" if the incident was a phishing success.

- *Policy or Procedure changes* – e.g. “Update the incident response plan to include ransomware payment guidelines” if that situation arose and wasn’t detailed; or “Add a procedure to involve the Facilities team if physical security is part of incident” etc. Possibly the incident reveals a need for a separate “Business Continuity/Disaster Recovery plan” if downtime was an issue.
- *Technical improvements* – e.g. “Implement centralized log monitoring (SIEM) by Q4 so that we catch issues faster” if detection was slow; or “Deploy encryption on all laptops” if a lost laptop wasn’t encrypted; or “Enable automatic cloud backups for critical files daily” if backup frequency was an issue.
- *Vendor changes* – maybe “Evaluate security of third-party file sharing tool or switch to a more secure alternative” if the breach came through a vendor.
- *Resource needs* – e.g. “Consider hiring a part-time security consultant or virtual CISO to assist in ongoing security compliance” if it was identified that in-house expertise is limited. Or budget for newer security software or an upgrade of the firewall, etc.
- *Test the plan* – If the incident showed confusion, perhaps plan additional drills. Actually, even if it went well, regular testing is wise. So an item could be “Schedule annual incident response tabletop exercise (next by March 2026) with a simulated breach scenario.”

Each action item is logged. The Incident Response Coordinator or a designated risk manager will track progress on these items and report to firm leadership. This ensures the lessons truly lead to improvements, rather than being forgotten.

- **Plan Update:** The Incident Response Plan document itself should be revised if necessary. If the incident exposed unclear instructions or missing sections, we update the plan accordingly. For example, if a new type of threat was encountered that we didn't have a playbook for, we might add a subsection addressing that scenario in the future. We will also update the contact list, roles, or any other information in the plan that was found outdated or incomplete. The updated plan should be re-approved by the firm's management and redistributed to all team members and stakeholders. (We maintain version control: e.g. "v1.1 updated after October 2025 incident, changes include X, Y, Z.")
- **Follow-up with Affected Parties:** Part of lessons learned is also externally focused. We should evaluate if our client notifications and support were adequate. For instance, if we offered credit monitoring, ensure clients actually received info to enroll. It might be appropriate to have partners reach out to key clients a few weeks later to reassure them and answer any lingering concerns. This is more of a client relationship task, but the plan can remind us to do so, to help rebuild trust. If regulators were involved (like the NY AG or HHS), be prepared to answer follow-up questions or undergo a

compliance review. We should incorporate any feedback from them into our improvements as well.

- **Document the Lessons:** Finally, document the outcome of the post-incident review – basically an **After-Action Report**. This could be an extension of the incident report or a separate memo. It should summarize what was learned and what will be done about it. This report can be used in future training (for example, to train new IRT members on past incidents) and is also evidence to regulators or auditors that the firm takes incidents seriously and continuously improves (e.g., a regulator will be interested to see that after a breach, the firm bolstered its safeguards). Under NY SHIELD Act, adjusting the security program based on lessons learned is explicitly expected, and this process fulfills that expectation.

By diligently reviewing and learning from each incident, the firm will enhance its security posture. Over time, the frequency and impact of incidents should decrease, and the response will become second-nature, thus better protecting our clients and the firm's practice.

10. Plan Review and Maintenance

(This is a short concluding section to reinforce how the plan stays current.)

This Incident Response Plan is a **living document**. To remain effective, it must be maintained and regularly tested:

- **Ownership:** The Incident Response Coordinator (or appointed Security Officer) is responsible for keeping the plan up to date. They will schedule an

annual review of the plan (at minimum) and also update it whenever there are significant changes in the firm's environment (like new IT systems, different office, new regulations) or after any major incident (as noted above).

- **<u>Annual Review</u>:** Each year (for example, every January), the IRT will convene to review this plan line by line. They will verify contact information, role assignments (accounting for staff turnover or new hires), and references to laws (ensuring no legal requirements have changed; e.g. if NY or federal law updates breach notice rules, incorporate the new rules). They will also incorporate any lessons from drills or minor incidents that occurred over the year. Any updates will be approved by the Managing Partner and communicated to the whole firm (at least to let everyone know of any procedural changes).
- **<u>Testing</u>:** The firm commits to testing the incident response plan regularly. This can be done via **tabletop exercises** – simulated incident scenarios where the IRT discusses what they would do, using this plan as a guide, to ensure the steps make sense and team members are familiar with their roles. For example, one year the scenario might be a ransomware attack on the file server, another year a lost smartphone with client data – covering different aspects. These exercises often reveal improvements or just keep everyone sharp. We will document the date and outcome of each test. Additionally, technical testing of backups (to ensure we can actually restore data) and of

security controls should be part of routine IT operations; that indirectly supports our incident readiness.

- **Training:** New employees (attorneys and staff alike) will receive an orientation on basic incident reporting: whom to call and the importance of quick action. Existing employees will get periodic refreshers, perhaps as part of annual compliance training, reminding them of their role in this plan. Key IRT members may attend specialized training (like SANS incident response courses or bar association CLEs on cybersecurity) to keep skills up and learn about evolving threats. Maintaining a level of cybersecurity literacy firm-wide is essential, as threats evolve (e.g., new phishing tactics, new compliance requirements like updated NYSBA guidelines).
- **Integration with Other Policies:** Ensure this plan aligns with other firm policies (like the disaster recovery plan, if any, or document retention policy). For instance, if the disaster recovery plan says backups are retained for X days, our IR plan should consider that in recovery. If we update password policy after an incident, reflect that in the IR plan references. Consistency avoids confusion during an incident.
- **Availability of Plan:** The plan must be easily accessible during an incident, including if IT systems are compromised. A printed copy should be stored securely in the office (perhaps in a known location like an emergency binder). An offline electronic copy (on a protected USB drive held by the Coordinator and Managing Partner, for example) is also useful. Key contact info from the

plan (phone numbers, etc.) might be stored in an IRT members' phones or wallets for quick access. In an emergency, no one should be scrambling to find the plan; they should know where it is.

- **Conclusion:** By following and maintaining this Incident Response Plan, DCH Law Firm demonstrates a commitment to protecting client data and responding effectively to any cybersecurity threats. The combination of preventive measures (firewalls, antivirus, 2FA, etc.) and this robust response procedure (as required by laws like the SHIELD Act) will significantly reduce risk. In the ever-evolving cyber landscape, preparedness and practice are key. This plan provides the firm with a clear roadmap to handle incidents in a way that minimizes harm, meets all legal duties (avoiding fines or penalties), and upholds the firm's professional reputation for confidentiality and integrity.

Appendix A: Incident Response Team Contact List

This appendix lists the key members of the Incident Response Team (IRT), their roles, contact information, and alternates. This list should be reviewed and updated quarterly or after staff changes.

Role	Name	Contact Information	Alternate (Name & Contact)
Incident Response Coordinator	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
IT Support / Technical Lead	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
Compliance & Privacy Officer	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
Managing Partner / Executive	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
Communications Coordinator	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
External Forensic Specialist (if retained)	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]
Cyber Insurance Contact (if applicable)	[Insert Name]	[Phone, Email, Mobile]	[Insert Alternate Info]

Appendix B: Incident Report Form

This form is to be completed for any suspected or confirmed security incident affecting XYZ Law Firm.

Date and Time of Report: ________________________________

Name of Reporter: ___________________________________

Contact Information: _________________________________

Department/Role: ____________________________________

Type of Incident (Check all that apply):

☐ Malware/Virus ☐ Phishing Email ☐ Unauthorized Access ☐ Lost/Stolen Device
☐ Data Breach ☐ System Outage ☐ Other: ______________

Describe the Incident (include what was observed, when it occurred, and any known impact):

Systems/Data Involved:

____

Immediate Actions Taken (if any):

Person Notified (Name & Time): ___________________________

Was the system removed from the network? ☐ Yes ☐ No

Other containment steps (if any): __________________________

Appendix C: Client Notification Template

[Client Name]

[Client Address]

Date: [Insert Date]

Subject: Notice of Data Security Incident

Dear [Client Name],

We are writing to inform you of a recent data security incident that may have involved your confidential information. On [insert date], our firm discovered [brief description of the nature of the incident]. We promptly initiated our incident response procedures, which included containment, investigation, and mitigation measures.

Based on our investigation, we determined that the information potentially involved included [types of information]. There is no indication at this time that the information has been misused; however, we are notifying you out of an abundance of caution and in accordance with our professional responsibility and applicable laws.

We have taken the following steps to address this issue: [list actions such as password resets, system updates, etc.]. We are also offering [credit monitoring, if applicable].

If you have any questions or concerns, please contact [Name, Title] at [phone number and email address].

We deeply regret any inconvenience or concern this may cause and remain committed to protecting your information.

Sincerely,

[Name]
[Title]
DCH Law Firm

Data Security Breach Notification Sample Letter

Sample letter from a breaching entity to notify New Yorkers of a Security Breach Incident

(Date)

Dear (name of person):
We are writing to inform you of a recent security incident at [name of organization]. This notification is sent pursuant to the New York State Information and Security Breach and Notification Act (General Business Law Section 899-aa or State
Technology Law Section 208).

[Describe what happened in general terms including the date of the security incident, specific categories of personal/
private information that were involved, what you are doing in response and inform the letter's recipient as to what they can do to protect themselves as indicated below.)

To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts,but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

- Equifax (888)766-0008 or www.fraudalert.equifax.com (https://www.fraudalert.equifax.com/)
- Experian (888) 397-3742 or www.experian.com (https://www.experian.com/)
- TransUnion (800) 680-7289 or www.transunion.com (https://www.transunion.com/)

New York residents can also consider placing a Security Freeze on their credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at https://dos.nysits.acsitefactory.com/consumer-protection (https://www.dos.ny.gov/consumerprotection/) .

When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com (https://www.annualcreditreport.com/) , calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm (https://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm) and mailing to:

Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283

For more information on identity theft, you can visit the following websites:
New York Department of State Division of Consumer Protection: www.dos.ny.gov/consumer-protection (https://dos.ny.gov/consumer-protection)
NYS Attorney General at: www.ag.ny.gov (https://ag.ny.gov/)
Federal Trade Commission
at: www.ftc.gov/bcp/edu/microsites/idtheft/ (https://www.ftc.gov/bcp/edu/microsites/idtheft/)

If there is anything [name of your organization and website] can do to further assist you, please call [name] and [phone number].

[Closing]

Please note: This sample letter from a breaching entity to notify New York residents of a security breach incident is for informational purposes only and should not be construed as legal advice and/or as policy of the State of New York. It is recommended that you speak with a privacy professional and/or an attorney for further advice.

Accessibility

Body Armor

Commissions & Committees

Community Services Block Grant

Disclaimer

Employment Opportunities

Meetings & Events

Executive Law 100-a

FOIL

Funding & Bid Opportunities

Language Access

Meeting Minutes

New New York Leaders

Office of Faith & Non-profit Development Services

Open Government

Pressroom

Privacy Policy

Site Map

State Register

Transparency Plan

Contact Us

Email Sign Up

CONNECT WITH US

FACEBOOK

TWITTER

KeyCite Yellow Flag
Proposed Legislation

McKinney's Consolidated Laws of New York Annotated
General Business Law (Refs & Annos)
Chapter 20. Of the Consolidated Laws
Article 39-F. Notification of Unauthorized Acquisition of Private Information; Data Security Protections (Refs & Annos)

McKinney's General Business Law § 899-aa

§ 899-aa. Notification; person without valid authorization has acquired private information

Currentness

1. As used in this section, the following terms shall have the following meanings:

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

(3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;

(4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical

characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

(6) medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(7) health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history, including but not limited to, appeals history; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, provided that such notification shall be made within thirty days after the breach has been discovered, except for the legitimate needs of law enforcement, as provided in subdivision four of this section.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately, provided that such notification shall be made within thirty days following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this article he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to twenty dollars per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within three years after either the date on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state, the division of state police, and the department of financial services as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons; provided, however, that notice to the department of financial services shall only be required if the person or business is a covered entity, as defined in 23 NYCRR 500.1, and provided further that such notice shall be provided to the department of financial services in compliance with 23 NYCRR 500.17. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (b) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for

Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

Credits

(Added L.2005, c. 442, § 4, eff. Dec. 7, 2005. Amended L.2005, c. 491, §§ 5 to 7, eff. Dec. 7, 2005; L.2011, c. 62, pt. A, § 43, eff. April 1, 2011; L.2013, c. 55, pt. N, § 6, eff. March 28, 2013; L.2019, c. 117, § 3, eff. Oct. 23, 2019; L.2024, c. 613, § 5, eff. March 21, 2025; L.2024, c. 647, §§ 1, 2, eff. Dec. 21, 2024; L.2025, c. 30, §§ 6, 7, eff. March 21, 2025; L.2025, c. 91, § 1, eff. Dec. 21, 2024.)

Notes of Decisions containing your search terms (0)
View all 3

McKinney's General Business Law § **899**-**aa**, NY GEN BUS § **899**-**aa**
Current through L.2025 chapters 1 to 49, 61 to 117. Some statute sections may be more current, see credits for details.

End of Document

Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist
Latest HIPAA Updates » HIPAA Training »

Delivered via email so please ensure you enter your email address correctly.

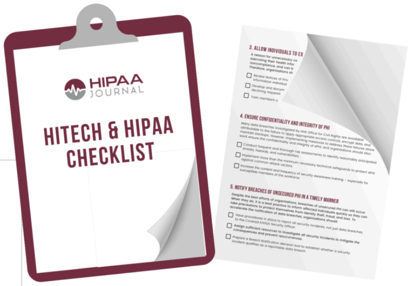
Your Privacy Respected
HIPAA Journal Privacy Policy

What is the HITECH Act?

Posted By Steve Alder on Jan 2, 2025

The Health Information Technology for Economic and Clinical Health Act or HITECH Act is the part of the American Recovery and Reinvestment Act of 2009 that incentivized the meaningful use of EHRs and strengthened the privacy and security provisions of HIPAA. Among other measures, the HITECH Act extended the reach of HIPAA to business associates of covered entities, who were now accountable for failures of HIPAA compliance. The Act also introduced tougher penalties for violations of HIPAA.

This article explains HITECH in depth. Get a copy of our **HITECH Act & HIPAA Checklist** to see the 20 ways The HITECH Act affected HIPAA and what is required for HIPAA Compliance.



Summary Of Article Contents

What are the Goals of the HITECH Act?

The five HITECH Act goals have been described as the five goals of the US healthcare system:

1. Improve quality, safety, and efficiency
2. Engage patients in their care
3. Increase coordination of care
4. Improve the health status of the population, and
5. Ensure privacy and security

To achieve these goals, HITECH incentivized the adoption and use of health information technology, enabled patients to take a proactive interest in their health, paved the way for the expansion of Health Information Exchanges, and strengthened the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HITECH also introduced tougher penalties for HIPAA compliance failures as extra incentive for healthcare organizations and their business associates to comply with the HIPAA Privacy and Security Rules and to fund increased enforcement action by the Department of Health and Human Services Office for Civil Rights.

The HITECH Act And ARRA

The HITECH Act of 2009, or Health Information Technology for Economic and Clinical Health Act, is part of the American Recovery and Reinvestment Act (ARRA) – an economic stimulus package introduced during the Obama administration.

ARRA had the objectives of:

- Promoting economic recovery by preserving and creating jobs
- Assisting those most impacted by the recession
- Investing in infrastructure such as transportation and environmental protection that would provide long-term benefits, and
- Stabilizing state and local government budgets.

A further objective helps define the purpose of the HITECH Act of 2009 – to provide investments needed to increase economic efficiency by spurring technological advances in science and health. To reach its objective, the HITECH Act had five goals.

Why is the HITECH Act Important?

Prior to the introduction of the HITECH Act in 2008, only 10% of hospitals had adopted EHRs. In order to advance healthcare, improve efficiency and care coordination, and make it easier for health information to be shared between covered entities, there needed to be an increase in EHR adoption and use.

While many healthcare providers wanted to transition to EHRs from paper records, the cost was prohibitively expensive. The HITECH Act introduced incentives to encourage hospitals and other healthcare providers to make the change. Had the Act not been passed, many healthcare providers would still be using paper records.

The HITECH Act also helped to ensure healthcare organizations and their business associates were complying with the HIPAA Privacy and Security Rules, were implementing safeguards to keep health information private and confidential, restricting uses and disclosures of health information, and were honoring their obligation to provide patients with copies of their medical records on request.

The Act did not make compliance with HIPAA mandatory as this was already a requirement, but it introduced a new requirement for covered entities and business associates to report data breaches – which ultimately enabled the Department of Human Services' Office for Civil Rights to step up enforcement action against non-compliant organizations.

© Copyright 2024 The HIPAA Journal. All rights reserved.

HITECH Act Summary

The HITECH Act encouraged healthcare providers to adopt electronic health records and improve privacy and security protections for healthcare data. This was achieved through financial incentives for adopting EHRs and increased penalties for violations of the HIPAA Privacy and Security Rules.

The HITECH Act contains four subtitles (A-D). Subtitle A concerns the promotion of health information technology and is split into two parts. Part 1 is concerned with improving healthcare quality, safety, and efficiency. Part 2 is concerned with the application and use of health information technology standards and reports.

Subtitle B covers testing of health information technology, Subtitle C covers grants and loans funding, and Subtitle D covers privacy and security of electronic health information. Subtitle D is also split into two parts. Part 1 is concerned with improving privacy and security of health IT and PHI, and Part 2 covers the relationship between the HITECH Act and other laws.

HITECH Act Compliance Date

The HITECH Act introduced a number of challenges for covered entities, business associates, and enforcement agencies such HHS' Office for Civil Rights and the Federal Trade Commission – which, under HITECH, is required to enforce the health breach notification regulations for vendors of personal health apps and other organizations not covered by HIPAA.

The compliance dates for HITECH were staggered. Some HITECH Act provisions – such as the authority for State Attorneys General to bring a civil action – were effective upon enactment (February 2009), while other provisions had effective dates 60 and 180 days after the passage of HITECH or by the end of the year.

The requirement for business associates to comply with HIPAA was scheduled to take effect in February 2010; but, as with many provisions of Subtitle D, some HITECH Act compliance dates were delayed until the publication of the HIPAA Final Omnibus Rule in 2013. As a result, there is no single HITECH Act compliance date.

The Meaningful Use Program

The Department of Health & Human Services (HHS) was given a budget in excess of $25 billion to achieve the goals of the HITECH Act. The HHS used some of that budget to fund the Meaningful Use program – a program that incentivized care providers to adopt certified EHRs by offering monetary incentives. Certified EHRs are those that have been certified as meeting defined standards by an authorized testing and certification body.

Certified EHRs had to be used in a meaningful way, such as for issuing electronic prescriptions and for the exchange of electronic health information to improve quality of care. The program aimed to improve coordination of care, improve efficiency, reduce costs, ensure privacy and security, improve population and public health, and engage patients and their caregivers more in their own healthcare.

The financial incentives were initially significant and increased with each year of the program as new requirements were introduced at each of the three stages of the Meaningful Use program. However, from 2015 onwards, Medicare-eligible professionals that did not comply with the HITECH EHR requirements saw the reimbursement of Medicare claims penalized by 1%. In 2017, the penalty for failing to demonstrate the adoption and use of a certified EHR increased to 3%.

How the HITECH Act of 2009 Forced Business Associates to be HIPAA Compliant

Under the original HIPAA Privacy and Security Rules, business associates of HIPAA covered entities had a "contractual obligation" to comply with HIPAA. Prior to the HITECH Act of 2009, there was no enforcement of that obligation, and covered entities could avoid sanctions in the event of a breach of PHI by a business associate by claiming they did not know the business associate was not HIPAA-compliant. Since business associates could not be fined directly for HIPAA violations, many failed to meet the standards demanded by HIPAA and were placing millions of health records at risk.

The HITECH Act of 2009 applied the HIPAA Security and Privacy Rules to business associates and made them directly liable for their own compliance with HIPAA. Business associates now had to sign a Business Associate Agreement with the covered entity on whose behalf they were processing PHI and had the same legal requirements as the covered entity to protect PHI and prevent data breaches. Business associates were also required to report data breaches to their covered entities.

The Omnibus HIPAA Final Rule of 2013 took business associates' compliance requirements a stage further. Following the enactment of the Omnibus HIPAA Final Rule, business associates were also subject to HIPAA audits and civil and criminal penalties could be issued directly to business associates for the failure to comply with HIPAA Rules and provide appropriate HIPAA training regardless of whether a data breach had occurred or not.

Tougher Penalties for HIPAA Violations

Prior to the introduction of the HITECH Act, as well as covered entities avoiding sanctions by claiming their business associates were unaware that they were violating HIPAA, the financial penalties HHS' Office for Civil Rights could impose were little more than a slap on the wrist ($100 for each violation up to a maximum fine of $25,000).

Tougher penalties were introduced for HIPAA violations in the HITECH Act and the penalties were split into different tiers based on different levels of culpability. The maximum financial penalty for a HIPAA violation was increased to $1.5 million per violation category, per year. Since 2016, HIPAA violation fines have been adjusted annually to account for inflation; and, as of December 2024, the maximum financial penalty per violation is now $2,134,831 per year.

Level of Culpability	Minimum Penalty per Violation Type	Maximum Penalty per Violation Type	Annual Penalty Limit
Lack of Knowledge	$141	$35,581	$35,581
Lack of Oversight	$1,424	$71,162	$142,355
Willful Neglect	$14,232	$71,162	$355,808
Willful Neglect not Corrected within 30 days	$71,162	$2,134,831	$2,134,831

Although civil monetary penalties for HIPAA violations go directly to the US Treasury, due to increased enforcement action since HITECH, HHS is able to go to Congress and justify requests for funding increases. With more resources available, HHS launched the first phase of its HIPAA compliance audit program in 2011. The second phase of 'desk audits' – paperwork checks – on covered entities was concluded in 2016, paving the way for a permanent audit program.

Amendment to HITECH Act 2021

In 2018, the Department for Health and Human services published a Request for Information with the objectives of exploring ways to reduce the administrative burden of HIPAA compliance and improve data sharing for better healthcare coordination. Many covered entities and business associates responded by requesting a safe harbor from enforcement action in the event of a data breach if they had complied with the safeguards of the HIPAA Security Rule.

As a result of the responses, an amendment to the HITECH Act in 2021 (also known as the HIPAA Safe Harbor law) gives the HHS' Office for Civil Rights the discretion to refrain from enforcement action, mitigate the degree of a penalty for violating HIPAA, or reduce the length of a Corrective Action Plan if the negligent party has implemented a recognized security framework and operated it for twelve months prior to a data breach or other security-related HIPAA violation.

The HIPAA Breach Notification Rule

An important change brought about by the passage of the HITECH Act was a new HIPAA Breach Notification Rule. Under the new HIPAA Breach Notification Rule, covered entities are required to issue notifications to affected individuals within sixty days of the discovery of a breach of unsecured Protected Health Information. The definition of "unsecured" was also clarified.

The breach notification letters to patients must be sent via first class mail and must explain the nature of the breach, the type(s) of Protected Health Information exposed or compromised, the steps that are being taken to address the breach, and the actions affected individuals can take to reduce the potential for harm.

Breaches of 500 or more records must also be reported to the HHS within 60 days of the discovery of a breach, and smaller breaches within 60 days of the end of the calendar year in which the breach occurred. In addition to reporting the breach to the HHS, a notice of a breach of 500 or more records must be provided to a prominent media outlet serving the state or jurisdiction affected by the breach.

The HIPAA Breach Notification Rule also requires business associates to notify their covered entities of a breach or HIPAA violation to allow the covered entity to report the incident to the HHS and arrange for individual notices to be sent.

Creation of the HIPAA Wall of Shame

The HITECH Act also called for the HHS' Office for Civil Rights (OCR) to start publishing a summary of healthcare data breaches that had been reported by HIPAA covered entities and their business associates. Starting in October 2009, OCR published breach summaries on its website, which included the name of the covered entity or business associate that experienced the breach, the category of the breach, the location of breached PHI, and the number of individuals affected.

The OCR breach portal earned the nickname 'The HIPAA Wall of Shame,' although the name is perhaps a little unfair as many entities listed have suffered breaches of PHI through no fault of their own.

Access to Electronic Health Records

The HIPAA Privacy Rule gave patients and health plan members a right of access and allowed them to obtain copies of information maintained in a designated record set. HITECH changed the HIPAA right of access standard so individuals could obtain a copy of their health data in electronic format if they so required. This change made it easier for individuals to share health data with other healthcare providers.

While it should be a relatively quick and easy process to provide electronic health records in electronic format, the reality is somewhat different. Some electronic health record systems make it difficult for health data to be provided in electronic format while some organizations may maintain multiple designated record sets about the same individual. To offset the costs of providing copies of electronic health records, healthcare organizations are permitted to charge a reasonable fee to cover the cost of labor for fulfilling the request.

Uses and Disclosures of Protected Health Information

The HITECH Act also made revisions to permitted uses and disclosures of PHI and tightened up the language of the HIPAA Privacy Rule. Covered entities are now prohibited from selling PHI or using it for fundraising or marketing without the written authorization of the patient or plan member. Patients and plan members have the right to revoke any authorizations they had previously given, and new requirements for accounting for disclosures of PHI and maintaining records of disclosures were introduced – including to whom PHI has been disclosed and for what purpose.

FAQs

How has the enforcement of HIPAA changed since the HITECH Act of 2009?

The enforcement of HIPAA changed since the HITECH Act of 2009 as the percentage of investigations resulting in enforcement action more than halved between 2013 and 2020. The reason for this appears to be that OCR intervened earlier in the complaints process and provided technical assistance to HIPAA covered entities, their business associates, and individuals exercising their rights under the HIPAA Privacy Rule to resolve complaints without the need for an investigation.

How did the burden of proof change under the HIPAA Breach Notification Rule?

The burden of proof changed under the HIPAA Breach Notification Rule because, prior to HITECH, when a violation of HIPAA occurred the Department of Health and Human Services had to prove the violation had resulted in the unauthorized disclosure of PHI. The HIPAA Breach Notification Rule reversed the burden of proof so that when a violation of HIPAA occurs the covered entity or business associate has to prove the violation did not result in the unauthorized disclosure of PHI.

How has HITECH evolved in recent years?

HITECH has evolved in recent years inasmuch as, in April 2018, CMS renamed the Meaningful Use incentive program as the Promoting Operability program. The change moved the focus of the program beyond the requirements of Meaningful Use to the interoperability of EHRs in order to improve data collection and submission, and patient access to health information.

Is the Promoting Operability program still incentivized?

The Promoting Operability program is still incentivized and now forms part of the Medicare Merit-Based Incentive Payment System (MIPS) which also measures the quality of healthcare services, the cost of healthcare services, and efforts to improve healthcare activities. The Promoting Operability category contributes to 25% of the overall MIPS score.

How do the Affordable Care Act and HITECH work together?

The Affordable Care Act and HITECH work together because the provisions of the HITECH Act that led to more efficient and secure information sharing enabled the expansion of state-run Health Information Exchanges (HIEs) as mandated by the Affordable Care Act. Originally, HIEs were intended to give consumers access to low-cost health insurance and Medicaid. They now also support the provision of coordinated care between providers.

What is HITECH in healthcare?

HITECH in healthcare can mean different things to different people depending on their place in the healthcare ecosystem. For example, for healthcare organizations, HITECH incentivized the adoption of EHRs. For business associates, HITECH in healthcare means they have to comply with the HIPAA Privacy and Security Rules when working with PHI on behalf of a covered entity, while for patients, HITECH in healthcare has mitigated the risk of a data breach and driven innovation in the healthcare industry.

Why was HITECH implemented and what were its results?

Primarily, HITECH was implemented to modernize the healthcare industry and make it more efficient while remaining secure. In terms of results, the Act increased the rate of EHR adoption throughout the healthcare industry from 3.2% in 2008 to 14.2% in 2015. By 2017, 86% of office-based physicians and 96% of non-federal acute care hospitals had adopted EHRs.

What did the HITECH Act do?

What the HITECH Act did was to revolutionize the way many healthcare facilities create, use, share, and maintain healthcare data. It made the health service more efficient, improved patient safety, and resulted in better patient outcomes according to a 2016 report to Congress by the National Coordinator for Health Information Technology.

What are the major components of the HITECH Act?

The major components of the HITECH Act are the Meaningful Use program and the provisions that were subsequently integrated into HIPAA. While the first component incentivized the adoption of health information technology, the second component encouraged covered entities and business associates to use the technology securely.

What is HITECH compliance?

The term HITECH compliance relates to complying with the provisions of HITECH that amended the HIPAA Privacy and Security Rules and complying with the HIPAA Breach Notification Rule that was implemented as a direct result of HITECH. A HITECH violation can also be a HIPAA violation – which can result in an OCR investigation, fine, and/or Corrective Order Plan being issued.

How did the HITECH Act modify HIPAA with regard to reporting data breaches?

The HITECH Act modified HIPAA with regards to reporting data breaches by introducing the HIPAA Breach Notification Rule. The Rule requires covered entities to report data breaches to affected individuals and HHS' Office for Civil Rights, and requires business associates to report all data breaches to the covered entity.

Prior to HITECH, HHS' Office for Civil Rights (OCR) most commonly learned about data breaches via patient complaints. Even then, OCR had to prove harm had occurred due to non-compliance with HIPAA, whereas now covered entities and business associates have the burden of proof to show harm has not occurred if not reporting a breach.

With HITECH, what other things were added to HIPAA?

With HITECH, the other things added to HIPAA (in addition to the HIPAA Breach Notification Rule) included tougher restrictions on the use of PHI for marketing and fundraising, the expansion of individuals' rights to restrict certain disclosures of PHI, additional uses and disclosures requiring an authorization, and the direct liability of business associates for violations of the HIPAA Privacy Rule (where provided), HIPAA Security Rule, and HIPAA Breach Notification Rule.

What is the HITECH Act in HIPAA?

The HITECH Act in HIPAA most often refers to the changes made to HIPAA by the passage of HITECH. However, it is important to be aware that the HITECH Act and HIPAA are two completely separate and independent laws. However, because some provisions of HITECH strengthened existing HIPAA standards and mandated breach notifications, HITECH is often (incorrectly) regarded as part of HIPAA. You can find out more about the relationship between the two Acts in this article.

What are the subtitles of HITECH?

The subtitles of HITECH are:

Subtitle A – Promotion of Health Information Technology

Subtitle B – Testing of Health Information Technology

Subtitle C – Grants and Loans Funding

Subtitle D – Privacy

What does the acronym HITECH stand for?

The acronym HITECH stands for Health Information Technology for Economic and Clinical Health. The content of the Act appears in two areas of ARRA – Division A Title XIII (Health Information Technology) and Division B Title IV (Medicare and Medicaid Health Information Technology; Miscellaneous Medicare provisions).

What is the HITECH Act of 2009?

The HITECH Act of 2009 is part of the American Recovery and Reinvestment Act (ARRA). It is responsible for the introduction of the Meaningful Use program to incentivize the adoption and use of health information technology. The HITECH Act also included measures that enabled individuals to take a proactive interest in their health, strengthened the privacy and security provisions of HIPAA, and required covered entities to notify individuals of data breaches.

What are the major components of the HITECH Act?

There are four major components of the HITECH Act. The first component (Subtitle A) is split into two parts – the first is related to improving healthcare quality, safety, and efficiency; the second part relates to the application and use of health information technology. The second component (Subtitle B) concerns the testing of health information technology, while the third component (Subtitle C) covers grants and funding for loans.

Subtitle D had the most significant impact on HIPAA, and many of its provisions related to improving the privacy and security of Protected Health Information were implemented via the HIPAA Final Omnibus Rule in 2013. Subtitle D is also where the HIPAA Breach Notification Rule, new regulations related to Business Associate Agreements, and increased criminal penalties for wrongful disclosures of individually identifiable health information can be found.

When was HITECH enacted?

HITECH was enacted in several stages. Some provisions were enacted at the time the HITECH Act was passed, and the majority of the HITECH regulations were enacted in 2011. However, many HITECH regulations contained in Subtitle D ("Privacy") were not enacted until 2013 when the Department of Health and Human Services published the HIPAA Final Omnibus Rule. A few provisions remain (for example 42 USC 17939 (c)(2) and (3)) that have still not been enacted.

Author: Steve Alder is the editor-in-chief of The HIPAA Journal. Steve is responsible for editorial policy regarding the topics covered in The HIPAA Journal. He is a specialist on healthcare industry legal and regulatory affairs, and has 10 years of experience writing about HIPAA and other related legal topics. Steve has developed a deep understanding of regulatory issues surrounding the use of information technology in the healthcare industry and has written hundreds of articles on HIPAA-related topics. Steve shapes the editorial policy of The HIPAA Journal, ensuring its comprehensive coverage of critical topics. Steve Alder is considered an authority in the healthcare industry on HIPAA. The HIPAA Journal has evolved into the leading independent authority on HIPAA under Steve's editorial leadership. Steve manages a team of writers and is responsible for the factual and legal accuracy of all content published on The HIPAA Journal. Steve holds a Bachelor's of Science degree from the University of Liverpool. You can connect with Steve via LinkedIn or email via stevealder(at)hipaajournal.com

About The HIPAA Journal

The HIPAA Journal provides the most comprehensive coverage of HIPAA news anywhere online, in addition to independent advice about HIPAA compliance and the best practices to adopt to avoid data breaches, HIPAA violations and regulatory fines. The HIPAA Journal's goal is to assist HIPAA-covered entities achieve and maintain compliance with state and federal regulations governing the use, storage and disclosure of PHI and PII.

Most Read Posts

- ComplianceJunction HIPAA Training Course Approved by AHIMA
- Exploit Released for 'PrintNightmare' Zero-Day Windows Print Spooler RCE Vulnerability
- NIST Publishes Critical Software Definition for U.S. Agencies
- NIST Releases Draft Guidance for Ransomware Risk Management

Click here to subscribe to free weekly newsletter

Advertise with The HIPAA Journal

Careers at The HIPAA Journal

Click here for LinkedIn
Click here for Twitter/X
Click here for Facebook

Submit Press Releases
Privacy Policy
Terms and Conditions
Trademark Policy
Accessibility Statement
Editorial Policy
Mission Statement

Copyright Policy (All Rights Reserved)

Cookie Policy

Site Map

HSS HIPAA link

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

United States Department of
Health & Human Services

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

OCR
OFFICE FOR CIVIL RIGHTS

HIPAA Compliance Assistance

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

SUMMARY OF
THE HIPAA PRIVACY RULE

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("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").[1] 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.

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.

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: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs.

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: http://www.hhs.gov/ocr/hipaa.

Statutory & Regulatory Background

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 *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within 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.[2]

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.[3] 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: http://www.hhs.gov/ocr/hipaa.

Who is Covered by the Privacy Rule

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: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities.[4] 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,[5] 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.

Health Care Providers. 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.[6] 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.

Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.[7] 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.[8] 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.

Business Associates

Business Associate Defined. 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.[9] 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.

Business Associate Contract. When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* 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.[10] 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.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html. Also see OCR "Business Associate" Guidance.

What Information is Protected

Protected Health Information. The Privacy Rule protects all *"individually identifiable health information"* 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 "*protected health information (PHI)*."[12]

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

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.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[14] 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.[15]

General Principle for Uses and Disclosures

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath 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.[16]

Required Disclosures. 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.[17] See OCR "Government Access" Guidance.

Permitted Uses and Disclosures

Permitted Uses and Disclosures. 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

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] 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.[19] 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.[20]
>
> ***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[21] 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.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

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.[24] 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.[25] 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. [26] 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.[27] 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.[28] 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).[29]

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.[30] 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.[31]

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.[32]

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.[33]

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.[34]

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.[35]

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.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] 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.[38] 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).[39] 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.[40]

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.[41]

Workers' Compensation. 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.[42] See OCR "Workers' Compensation" Guidance.

(6) Limited Data Set. 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.[43] 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.

Authorized Uses and Disclosures

Authorization. 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.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45]

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.

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.[46]

Psychotherapy Notes[47]. A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]:

- The covered entity who originated the notes may use them for treatment.
- 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.

Marketing. Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;

- 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;
- Communications for treatment of the individual; and
- 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.

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 OCR "Marketing" Guidance.

Limiting Uses and Disclosures to the Minimum Necessary

Minimum Necessary. 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.[50] 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 OCR "Minimum Necessary" Guidance.

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.

Access and Uses. 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 protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

Disclosures and Requests for Disclosures. Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* 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.

Reasonable Reliance. 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.

Notice and Other Individual Rights

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] 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 OCR "Notice" Guidance.

- **Notice Distribution.** A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows:
  - 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);
  - 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
  - In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] 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.[53] 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.[54] 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*.[55] 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.[56] 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.[57] 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.[58] 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.[59] 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.[60] 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.[61] 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.[62]

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.[63] 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.[64]

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.[65]

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).[66] 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.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68]

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.[69]

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.[70] 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.[71] The covered entity must explain those procedures in its privacy practices notice.[72]

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.[73] A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74]

Documentation and Record Retention. 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.[75]

Fully-Insured Group Health Plan Exception. 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.[76]

Organizational Options

The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections.

Hybrid Entity. 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."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) 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.

Affiliated Covered Entity. 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.[79] 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.

Organized Health Care Arrangement. 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."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81]

Covered Entities With Multiple Covered Functions. 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.[82] 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.

Group Health Plan disclosures to Plan Sponsors. 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[83]:

- Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan.
- 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).
- 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.

Other Provisions: Personal Representatives and Minors

Personal Representatives. The Privacy Rule requires a covered entity to treat a *"personal representative"* 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.[84] 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.

Special case: Minors. 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 OCR "Personal Representatives" Guidance.

State Law

Preemption. 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.[85] "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.[86] 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.

Exception Determination. 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:

- Is necessary to prevent fraud and abuse related to the provision of or payment for health care,
- Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
- Is necessary for State reporting on health care delivery or costs,
- 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
- 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.

Enforcement and Penalties for Noncompliance

Compliance. 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.[87] 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.

Civil Money Penalties. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] 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.

Criminal Penalties. 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.[89] 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.

Compliance Dates

Compliance Schedule. All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply.

Small Health Plans. A health plan with annual receipts of not more than $5 million is a small health plan.[91] 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.[92]
See What constitutes a small health plan?

Copies of the Rule & Related Materials

The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] 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.

[6] 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.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] 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).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] 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.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 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).

[44] 45 C.F.R. § 164.508.

[45] 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).

[46] 45 CFR § 164.532.

[47] "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.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 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.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] 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.

[58] 45 C.F.R. § 164.526.

[59] 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).

[60] 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 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.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 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.

[80] 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.

[81] 45 C.F.R. § 164.506(c)(5).

[82] 45 C.F.R. § 164.504(g).

[83] 45 C.F.R. § 164.504(f).

[84] 45 C.F.R. § 164.502(g).

[85] 45 C.F.R. §160.203.

[86] 45 C.F.R. § 160.202.

[87] 45 C.F.R.§ 160.304

[88] Pub. L. 104-191; 42 U.S.C. §1320d-5.

[89] Pub. L. 104-191; 42 U.S.C. §1320d-6.

[90] 45 C.F.R. § 164.534.

[91] 45 C.F.R. § 160.103.

[92] 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.

U.S. Department of
Health and Human Services
Enhancing the health and well-being of all Americans

HHS </> HIPAA Home </hipaa/index.html> For Professionals </hipaa/for-professionals/index.html> Covered Entities and …

Navigate to:

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity’s obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS 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 for purposes of HHS determining the covered entity’s compliance with the

HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual’s request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual’s request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “covered entity” or “individual”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.”]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity’s minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity’s minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate’s use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate’s use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate’s use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Learn more about business associates <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

Back to Top

Guidance Materials for Covered Entities

- Summary of the Privacy Rule </ocr/privacy/hipaa/understanding/summary/index.html>
- Guidance on Significant Aspects of the Privacy Rule </ocr/privacy/hipaa/understanding/coveredentities/privacyguidance.html>
- Fast Facts for Covered Entities </ocr/privacy/hipaa/understanding/coveredentities/cefastfacts.html>

- Provider Guide: Communicating With a Patient's Family, Friends, or Other Persons Identified by the Patient [PDF, 60 KB] </sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf>
- Guidance on the Application of FERPA and HIPAA to Student Health Records [PDF, 294 KB] </sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf>
- Sample Business Associate Contract </ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>
- Misleading Marketing Claims </ocr/privacy/hipaa/understanding/coveredentities/misleadingmarketing.html>
- Sign Up for the OCR Privacy Listserv </ocr/privacy/hipaa/understanding/coveredentities/listserv.html>

Content created by Office for Civil Rights (OCR)
Content last reviewed June 16, 2017

Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018)

American Bar Association

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers’ Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), https://www.cio.com (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); *See also Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, Cyber Division (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, Wall St. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,[6] and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.[7]

[6] The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

[7] In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g.*, *Cybersecurity Resources*, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”[8] The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[9]

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document. [10]

[8] MODEL RULES OF PROF’L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[10] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[11]

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).

[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").

[14] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF'L CONDUCT R. 1.15 (2018).

[15] *See also* MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2018).

[16] The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); *See also* National Cyber Security Centre "Ten Steps to Cyber Security" [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.[18] The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. "One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents."[19] While every lawyer's response plan should be tailored to the lawyer's or the law firm's specific practice, as a general matter incident response plans share common features:

> The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

[18] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting "an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.").
[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.[20]

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[21] These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

[21] We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).[22] Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[23] The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[24]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

[22] The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

[24] *Id.* at (c).

- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[25]

As this Committee recognized in ABA Formal Opinion 477R:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.[26] Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.[27] As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[28]

[25] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2018). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

[26] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

[27] MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. [18] (2018) ("The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.")

[28] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.[29] In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.[30] We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.[31]

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[30] This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

[31] Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: "If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach."[32] The Committee advised:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).[33]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.[34]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[33] *Id.*

[34] MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property." Funds must be kept in a separate account, and "[o]ther property shall be identified as such and appropriately safeguarded." Model Rule 1.15(a) also provides that, "Complete records of such account funds and other property shall be kept by the lawyer . . . ." Comment [1] to Model Rule 1.15 states:

> A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form. Comment [1] uses as examples "securities" and "property" that should be kept separate from the lawyer's "business and personal property." That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15's safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, "Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information."

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client."[35] When electronic "information relating to the representation" of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the former client. Rule 1.9(c) provides that a lawyer "shall not . . . reveal" the former client's information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] We also note that Rule 1.16(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.[38] Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).

[36] *See* Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent's argument that the court should engraft an additional element of proof in a disciplinary charge because "such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.").

[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).

[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.[39]

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

[39] *Cf.* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.[40] Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] *Id.*
[43] *Id.*
[44] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.
[45] Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

2023 New York Statewide Civil Legal Aid Technology Conference

2A Agents of the SHIELD - Data Privacy and Security
Wednesday, April 19, 2023
1:00 PM – 1:50 PM
Live Virtual Presentation
CLE Credits: 1.0 Cybersecurity, Privacy and Data-Ethics

CLE Resources

Stop Hacks and Improve Electronic Data Security Act (“Shield Act”)

NY State Senate Bill S5575

New York Rules of Professional Conduct 1.1, 1.4, 1.6, 5.1, 5.2, 5.3

ABA Formal Opinion 477R: Securing Communication of Protected Client Information

ABA Formal Opinion 483: Lawyers’ Obligations After an Electronic Data Breach of Cyberattack

ABA Formal Opinion 498: Virtual Practice

NYSBA Ethics Opinion 1240: Duty to Protect Client Information Stored on a Lawyer’s Smartphone

NYSBA Ethics Opinion 1019: Confidentiality; Remote Access to Firm’s Electronic Files

NYSBA Ethics Opinion 842: Using an Outside Storage Provider to Store Client Confidential Information

New York State Continuing Legal Education Requirements: Cybersecurity, Privacy and Data Protection FAQs

Supplemental Materials

Agents of the SHIELD - Data Privacy and Security | Cybersecurity, Privacy and Data-Ethics CLE

Moderator: Amber Wilder, Associate Project Manager, Just-Tech

Speakers: Sandy Coyne, Deputy Director of Operations; Lori M. O'Brien, Esq., Deputy Director, Legal Assistance of Western New York, Inc.; Ellen Samuel, Director of Consulting, Just-Tech

Description: The presenters will discuss practical steps to bring your organization into compliance with the New York State Shield Act and reduce the risk of confidential data compromise. Presenters will discuss the ethics of cybersecurity, including a lawyer's duty of technological competence, protecting client confidentiality, and supervising third-party service providers. This session will include a discussion of security incidents involving legal aid organizations and how compliance with the Shield Act and other cybersecurity best practices would reduce the fall-out from such incidents.

Stop Hacks and Improve Electronic Data Security Act (“SHIELD Act”)

What is the significance of this law?

The SHIELD Act, signed into law on July 25, 2019 by Governor Andrew Cuomo, amends New York’s 2005 Information Security Breach and Notification Act. The Shield Act significantly strengthens New York’s data security laws by expanding the types of private information that companies must provide consumer notice in the event of a breach, and requiring that companies develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.

What types of security breaches are covered by this law?

Under the 2005 law, a security breach is defined as an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of private information. The SHIELD Act expands the definition of a security breach to any “access” to computerized data that compromises the confidentiality, security, or integrity of private data.

What does private information consist of?

Under the 2005 law, private information was any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver’s license number, account number, or credit or debit card number in combination with any required security code. The SHIELD Act expands the law to include biometric information, and username/email address and password credentials.

What are the safeguards that are included in the SHIELD Act?

The SHIELD Act requires any person or business that maintains private information to adopt administrative, technical and physical safeguards. Certain safeguards are listed but it is not meant to be an exhaustive list.

Reasonable administrative safeguards:

- designates one or more employees to coordinate the security program;
- identifies reasonably foreseeable internal and external risks;
- assesses the sufficiency of safeguards in place to control the identified risks;
- trains and manages employees in the security program practices and procedures;
- selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
- adjusts the security program in light of business changes or new circumstances.

Reasonable technical safeguards:

- assesses risks in network and software design;
- assesses risks in information processing, transmission and storage;
- detects, prevents and responds to attacks or system failures; and
- regularly tests and monitors the effectiveness of key controls, systems and procedures.

Reasonable physical safeguards:

- assesses risks of information storage and disposal;
- detects, prevents and responds to intrusions;
- protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

What are the obligations of businesses when a breach occurs?

The law requires that the person or business notify the affected consumers following discovery of the breach in the security of its computer data system affecting private information. The disclosure must be made in the most expedient time possible consistent with legitimate needs of law enforcement agencies. While the law requires notice to the Attorney General's office, New York Department of State and the New York State Police of the timing, content and distribution of the notices and approximate number of affected persons, submission of a breach form through the NYAG data breach reporting portal is sufficient as its automatically sent to all three entities: • Data Breach Reporting Portal

The person or business must also notify consumer reporting agencies if more than 5,000 New York residents are to be notified. The contact information for the three nationwide consumer reporting agencies is as follows:

EQUIFAX
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
www.equifax.com

EXPERIAN
Consumer Fraud Assistance
P.O. Box 9554
Allen, TX 75013
888-397-3742

www.experian.com

TRANSUNION
P.O. Box 2000
Chester, PA 19016-2000
Phone: 800-909-8872
www.transunion.com

If you are a consumer affected by a breach, you may **file a complaint through the Attorney General’s online complaint form**. Do not submit a breach notification form.

Are there any exceptions to the notification requirements?

The law also provides for substitute notice to consumers if the business demonstrates to the Attorney General that the cost of providing regular notice would exceed $250,000 or that the affected class of persons exceeds 500,000 or the entity or business does not have sufficient contact information. Where substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity’s web site, and notification to statewide media.

The law also does not require consumer notification if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

What are the penalties for violations of the SHIELD Act?

Under the SHIELD Act, the Attorney General may seek injunctive relief, restitution and penalties against any business entity for violating the law. For failure to provide timely notification, the court may impose a civil penalty of up to $20 per instance of failed notification not to exceed $250,000. For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to $5,000 per violation.

Bureau of Internet and Technology (BIT)

- Resource Center
  - File a Complaint
  - Consumer Education

  - Privacy and Identity Theft
  - Child Safety
  - Buying Online
  - Common Online Scams

- Report a Data Security Breach
- ▾ Initiatives
  - Anti-Child Pornography Initiatives
  - Electronic Security and Targeting of Online Predators Act (e-STOP)
  - Operation: Game Over
  - Report: Obstructed View: What’s Blocking New Yorkers from Getting Tickets
  - Report: Airbnb in the city
  - Safety Model for Social Networking Sites

- Press Releases
- Contact

Search:

Please enter a search term...

STATE OF NEW YORK

5575--B

Cal. No. 1094

2019-2020 Regular Sessions

IN SENATE

May 7, 2019

Introduced by Sens. THOMAS, CARLUCCI, BIAGGI -- (at request of the Attorney General) -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged and said bill committed to the Committee on Consumer Protection -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, passed by Senate and delivered to the Assembly, recalled, vote reconsidered, restored to third reading, amended and ordered reprinted, retaining its place in the order of third reading

AN ACT to amend the general business law and the state technology law, in relation to notification of a security breach

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)".

§ 2. The article heading of article 39-F of the general business law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE
INFORMATION**; DATA SECURITY PROTECTIONS**

§ 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899-aa of the general business law, subdivisions 1, 2, 3, 5, 6 and 7 as added by chapter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9 is renumbered subdivision 10 and a new subdivision 9 is added to read as follows:

1. As used in this section, the following terms shall have the following meanings:

EXPLANATION--Matter in **italics** (underscored) is new; matter in brackets [-] is old law to be omitted.

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information [~~or~~] plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; [~~or~~]

(3) account number, credit or debit card number, in combination with any required security code, access code, [~~or~~] password or other information that would permit access to an individual's financial account;

(4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of [~~personal~~] private information maintained by a business. Good faith access to, or acquisition of [~~personal~~], private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which [~~conducts business in New York state, and which~~] owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, **accessed or** acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the system.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this article he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to [~~ten~~] twenty dollars per instance of failed notification, provided that the latter amount shall not exceed [~~one~~] two hundred fifty thousand dollars.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within [~~two~~] three years [~~immediately~~]

after either the date [~~of the act complained of or the date of discovery of such act~~] on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (b) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

§ 4. The general business law is amended by adding a new section 899-bb to read as follows:

§ 899-bb. Data security protections. 1. Definitions. (a) "Compliant regulated entity" shall mean any person or business that is subject to, and in compliance with, any of the following data security requirements:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

(b) "Private information" shall have the same meaning as defined in section eight hundred ninety-nine-aa of this article.

(c) "Small business" shall mean any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.

(b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either:

(i) is a compliant regulated entity as defined in subdivision one of this section; or

(ii) implements a data security program that includes the following:

(A) reasonable administrative safeguards such as the following, in which the person or business:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

(4) trains and manages employees in the security program practices and procedures;

(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and

(6) adjusts the security program in light of business changes or new circumstances; and

(B) reasonable technical safeguards such as the following, in which the person or business:

(1) assesses risks in network and software design;

(2) assesses risks in information processing, transmission and storage;

(3) detects, prevents and responds to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and

(C) reasonable physical safeguards such as the following, in which the person or business:

(1) assesses risks of information storage and disposal;

(2) detects, prevents and responds to intrusions;

(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

(4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

(c) A small business as defined in paragraph (c) of subdivision one of this section complies with subparagraph (ii) of paragraph (b) of subdivision two of this section if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers.

(d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fifty-d of this chapter.

(e) Nothing in this section shall create a private right of action.

§ 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8 of section 208 of the state technology law, paragraph (a) of subdivision 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005, subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as amended by chapter 491 of the laws of 2005, are amended and a new subdivision 9 is added to read as follows:

(a) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information [~~or~~] plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; [~~or~~]

(3) account number, credit or debit card number, in combination with any required security code, access code, [~~or~~] password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a

report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the

notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. **The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.**

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

§ 6. This act shall take effect on the ninetieth day after it shall have become a law; provided, however, that section four of this act shall take effect on the two hundred fortieth day after it shall have become a law.

RULE 1.1

COMPETENCE

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter, and whether it is feasible to associate with a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances. One such circumstance would be where the lawyer, by representations made to the client, has led the client reasonably to expect a special level of expertise in the matter undertaken by the lawyer.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all

legal problems. Perhaps the most fundamental legal skill consists of determining what kinds of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] [Reserved.]

[4] A lawyer may accept representation where the requisite level of competence can be achieved by adequate preparation before handling the legal matter. This applies as well to a lawyer who is appointed as counsel for an unrepresented person.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client may limit the scope of the representation if the agreement complies with Rule 1.2(c).

Retaining or Contracting with Lawyers Outside the Firm

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and should reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. *See also* Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(g) (fee sharing with lawyers outside the firm), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the needs of the client; the education, experience and reputation of the outside lawyers; the nature of the services assigned to the outside lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[6A] Client consent to contract with a lawyer outside the lawyer's own firm may not be necessary for discrete and limited tasks supervised closely by a lawyer in the firm. However, a lawyer should ordinarily obtain client consent before contracting with an outside lawyer to perform substantive or strategic legal work on which the lawyer will exercise independent judgment without close supervision or review by the referring lawyer. For example, on one hand, a lawyer who hires an outside lawyer on a per diem basis to cover a single court call or a routing calendar call ordinarily would not need to obtain the client's prior informed consent. On the other hand, a lawyer who hires an outside lawyer to argue a summary judgment motion or negotiate key points in a transaction ordinarily should seek to obtain the client's prior informed consent.

[7] When lawyer from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other about the scope of their respective roles and the allocation of responsibility among them. *See* Rule 1.2(a). When allocating responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations (*e.g.*, under local court rules, the CPLR, or the Federal Rules of Civil Procedure) that are a matter of law beyond the scope of these Rules.

[7A] Whether a lawyer who contracts with a lawyer outside the firm needs to obtain informed consent from the client about the roles and responsibilities of the retaining and outside lawyers will depend on the circumstances. On one hand, if a lawyer retains an outside lawyer or law firm to work under the lawyer's close direction and supervision, and the retaining lawyer closely reviews the outside lawyer's work, the retaining lawyer usually will not need to consult with the client about the outside lawyer's role and level of responsibility. On the other hand, if the outside lawyer will have a more material role and will exercise more autonomy and responsibility, then the retaining lawyer usually should consult with the client. In any event, whenever a retaining lawyer discloses a client's confidential information to lawyers outside the firm, the retaining lawyer should comply with Rule 1.6(a).

[8] To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

RULE 1.4

COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of:

(i) any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required by these Rules;

(ii) any information required by court rule or other law to be communicated to a client; and

(iii) material developments in the matter including settlement or plea offers.

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with a client's reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by these Rules or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client to participate effectively in the representation.

Communicating with Client

[2] In instances where these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with the client and secure the

client's consent prior to taking action, unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, paragraph (a)(1)(iii) requires that a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously made clear that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. *See* Rule 1.2(a).

[3] Paragraph (a)(2) requires that the lawyer reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases, the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Likewise, for routine matters such as scheduling decisions not materially affecting the interests of the client, the lawyer need not consult in advance, but should keep the client reasonably informed thereafter. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer or a member of the lawyer's staff acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications, or arrange for an appropriate person who works with the lawyer to do so.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should

review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interest and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(j).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. *See* Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to those who the lawyer reasonably believes to be appropriate persons within the organization. *See* Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

RULE 1.6

CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Comment

Scope of the Professional Duty of Confidentiality

[1] This Rule governs the disclosure of information protected by the professional duty of confidentiality. Such information is described in these Rules as "confidential information" as defined in this Rule. Other rules also deal with confidential information. See Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients; Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client; Rule 1.14(c) for information relating to representation of a client with diminished capacity; Rule 1.18(b) for the lawyer's duties with respect to information provided to the lawyer by a prospective client; Rule 3.3 for the lawyer's duty of candor to a tribunal; and Rule 8.3(c) for information gained by a lawyer or judge while participating in an approved lawyer assistance program.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source. See Rule 1.0(j) for the definition of informed consent. The lawyer's duty of confidentiality contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer,

even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Typically, clients come to lawyers to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is thereby upheld.

[3] The principle of client-lawyer confidentiality is given effect in three related bodies of law: the attorney-client privilege of evidence law, the work-product doctrine of civil procedure and the professional duty of confidentiality established in legal ethics codes. The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information or evidence concerning a client. The professional duty of client-lawyer confidentiality, in contrast, applies to a lawyer in all settings and at all times, prohibiting the lawyer from disclosing confidential information unless permitted or required by these Rules or to comply with other law or court order. The confidentiality duty applies not only to matters communicated in confidence by the client, which are protected by the attorney-client privilege, but also to all information gained during and relating to the representation, whatever its source. The confidentiality duty, for example, prohibits a lawyer from volunteering confidential information to a friend or to any other person except in compliance with the provisions of this Rule, including the Rule's reference to other law that may compel disclosure. *See* Comments [12]-[13]; *see also* Scope.

[4] Paragraph (a) prohibits a lawyer from knowingly revealing confidential information as defined by this Rule. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal confidential information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation with persons not connected to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client.

[4A] Paragraph (a) protects all factual information "gained during or relating to the representation of a client." Information relates to the representation if it has any possible relevance to the representation or is received because of the representation. The accumulation of legal knowledge or legal research that a lawyer acquires through practice ordinarily is not client information protected by this Rule. However, in some circumstances, including where the client and the lawyer have so agreed, a client may have a proprietary interest in a particular product of the lawyer's research. Information that is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not "generally known" simply because it is in the public domain or available in a public file.

Use of Information Related to Representation

[4B] The duty of confidentiality also prohibits a lawyer from using confidential information to the advantage of the lawyer or a third person or to the disadvantage of a client or former client unless the client or former client has given informed consent. See Rule 1.0(j) for the definition of "informed consent." This part of paragraph (a) applies when information is used to benefit either the lawyer or a third person, such as another client, a former client or a business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not (absent the client's informed consent) use that information to buy a nearby parcel that is expected to appreciate in value due to the client's purchase, or to recommend that another client buy the nearby land, even if the lawyer does not reveal any confidential information. The duty also prohibits disadvantageous use of confidential information unless the client gives informed consent, except as permitted or required by these Rules. For example, a lawyer assisting a client in purchasing a parcel of land may not make a competing bid on the same land. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client, even to the disadvantage of the former client, after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(1).

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer may make disclosures of confidential information that are impliedly authorized by a client if the disclosures (i) advance the best interests of the client and (ii) are either reasonable under the circumstances or customary in the professional community. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. In addition, lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has

instructed that particular information be confined to specified lawyers. Lawyers are also impliedly authorized to reveal information about a client with diminished capacity when necessary to take protective action to safeguard the client's interests. See Rules 1.14(b) and (c).

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions that prevent substantial harm to important interests, deter wrongdoing by clients, prevent violations of the law, and maintain the impartiality and integrity of judicial proceedings. Paragraph (b) permits, but does not require, a lawyer to disclose information relating to the representation to accomplish these specified purposes.

[6A] The lawyer's exercise of discretion conferred by paragraphs (b)(1) through (b)(3) requires consideration of a wide range of factors and should therefore be given great weight. In exercising such discretion under these paragraphs, the lawyer should consider such factors as: (i) the seriousness of the potential injury to others if the prospective harm or crime occurs, (ii) the likelihood that it will occur and its imminence, (iii) the apparent absence of any other feasible way to prevent the potential injury, (iv) the extent to which the client may be using the lawyer's services in bringing about the harm or crime, (v) the circumstances under which the lawyer acquired the information of the client's intent or prospective course of action, and (vi) any other aggravating or extenuating circumstances. In any case, disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to prevent the threatened harm or crime. When a lawyer learns that a client intends to pursue or is pursuing a course of conduct that would permit disclosure under paragraphs (b)(1), (b)(2) or (b)(3), the lawyer's initial duty, where practicable, is to remonstrate with the client. In the rare situation in which the client is reluctant to accept the lawyer's advice, the lawyer's threat of disclosure is a measure of last resort that may persuade the client. When the lawyer reasonably believes that the client will carry out the threatened harm or crime, the lawyer may disclose confidential information when permitted by paragraphs (b)(1), (b)(2) or (b)(3). A lawyer's permissible disclosure under paragraph (b) does not waive the client's attorney-client privilege; neither the lawyer nor the client may be forced to testify about communications protected by the privilege, unless a tribunal or body with authority to compel testimony makes a determination that the crime-fraud exception to the privilege, or some other exception, has been satisfied by a party to the proceeding. For a lawyer's duties when representing an organizational client engaged in wrongdoing, see Rule 1.13(b).

[6B] Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial risk that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims. Wrongful execution of a person is a life-threatening and imminent harm under paragraph (b)(1) once the person has been convicted and sentenced to death. On the other hand, an event that will cause property damage but is unlikely to cause substantial bodily harm is not a present and substantial risk under paragraph (b)(1); similarly, a remote possibility or small statistical likelihood that any particular unit of a mass-distributed product will cause death or substantial bodily harm to unspecified persons over a period of years does not satisfy the element of reasonably certain death or substantial bodily harm under the exception to the duty of confidentiality in paragraph (b)(1).

[6C] Paragraph (b)(2) recognizes that society has important interests in preventing a client's crime. Disclosure of the client's intention is permitted to the extent reasonably necessary to prevent the crime. In exercising discretion under this paragraph, the lawyer should consider such factors as those stated in Comment [6A].

[6D] Some crimes, such as criminal fraud, may be ongoing in the sense that the client's past material false representations are still deceiving new victims. The law treats such crimes as continuing crimes in which new violations are constantly occurring. The lawyer whose services were involved in the criminal acts that constitute a continuing crime may reveal the client's refusal to bring an end to a continuing crime, even though that disclosure may also reveal the client's past wrongful acts, because refusal to end a continuing crime is equivalent to an intention to commit a new crime. Disclosure is not permitted under paragraph (b)(2), however, when a person who may have committed a crime employs a new lawyer for investigation or defense. Such a lawyer does not have discretion under paragraph (b)(2) to use or disclose the client's past acts that may have continuing criminal consequences. Disclosure is permitted, however, if the client uses the new lawyer's services to commit a further crime, such as obstruction of justice or perjury.

[6E] Paragraph (b)(3) permits a lawyer to withdraw a legal opinion or to disaffirm a prior representation made to third parties when the lawyer reasonably believes that third persons are still relying on the lawyer's work and the work was based on "materially inaccurate information or is being used to further a crime or fraud." *See* Rule 1.16(b)(1), requiring the lawyer to withdraw when the lawyer knows or reasonably should know that the representation will result in a violation of law. Paragraph (b)(3) permits the lawyer to give only the limited notice that is implicit in withdrawing an opinion or representation, which may have the collateral effect of inferentially revealing confidential information. The lawyer's withdrawal of the tainted opinion or representation allows the lawyer to prevent further harm to third persons and to protect the lawyer's own interest when the client has abused the professional relationship, but paragraph (b)(3) does not permit explicit disclosure of the client's past acts unless such disclosure is permitted under paragraph (b)(2).

[7] [Reserved.]

[8] [Reserved.]

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about compliance with these Rules and other law by the lawyer, another lawyer in the lawyer's firm, or the law firm. In many situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with these Rules, court orders and other law.

[10] Where a claim or charge alleges misconduct of the lawyer related to the representation of a current or former client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. Such a claim can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, such as a person claiming to have been defrauded by the lawyer and client acting together or by the lawyer acting alone. The lawyer may respond directly to the person who has made an accusation that permits disclosure, pro-

vided that the lawyer's response complies with Rule 4.2 and Rule 4.3, and other Rules or applicable law. A lawyer may make the disclosures authorized by paragraph (b)(5) through counsel. The right to respond also applies to accusations of wrongful conduct concerning the lawyer's law firm, employees or associates.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Paragraph (b) does not mandate any disclosures. However, other law may require that a lawyer disclose confidential information. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of confidential information appears to be required by other law, the lawyer must consult with the client to the extent required by Rule 1.4 before making the disclosure, unless such consultation would be prohibited by other law. If the lawyer concludes that other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

[13] A tribunal or governmental entity claiming authority pursuant to other law to compel disclosure may order a lawyer to reveal confidential information. Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason. In the event of an adverse ruling, the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge, unless such consultation would be prohibited by other law. If such review is not sought or is unsuccessful, paragraph (b)(6) permits the lawyer to comply with the order.

[14] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified in paragraphs (b)(1) through (b)(6). Before making a disclosure, the lawyer should, where practicable, first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose, particularly when accusations of wrongdoing in the representation of a client

have been made by a third party rather than by the client. If the disclosure will be made in connection with an adjudicative proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know the information, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[15] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may, however, be required by other Rules or by other law. *See* Comments [12]-[13]. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). *E.g.*, Rule 8.3(c)(1). Rule 3.3(c), on the other hand, requires disclosure in some circumstances whether or not disclosure is permitted or prohibited by this Rule.

Withdrawal

[15A] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw pursuant to Rule 1.16(b)(1). Withdrawal may also be required or permitted for other reasons under Rule 1.16. After withdrawal, the lawyer is required to refrain from disclosing or using information protected by Rule 1.6, except as this Rule permits such disclosure. Neither this Rule, nor Rule 1.9(c), nor Rule 1.16(e) prevents the lawyer from giving notice of the fact of withdrawal. For withdrawal or disaffirmance of an opinion or representation, see paragraph (b)(3) and Comment [6E]. Where the client is an organization, the lawyer may be in doubt whether the organization will actually carry out the contemplated conduct. Where necessary to guide conduct in connection with this Rule, the lawyer may, and sometimes must, make inquiry within the organization. *See* Rules 1.13(b) and (c).

Duty to Preserve Confidentiality

[16] Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to

current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients. Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.,* by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule. For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked "Confidential" or "Confidential—Attorneys' Eyes Only"; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.

Lateral Moves, Law Firm Mergers, and Confidentiality

[18A] When lawyers or law firms (including in-house legal departments) contemplate a new association with other lawyers or law firms though lateral hiring or merger, disclosure of limited information may be necessary to resolve conflicts of interest pursuant to Rule 1.10 and to address financial, staffing, operational, and other practical issues. However, Rule 1.6(a) requires lawyers and law firms to protect their clients' confidential information, so lawyers and law firms may not disclose such information for their own advantage or for the advantage of third parties absent a client's informed consent or some other exception to Rule 1.6.

[18B] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter, including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each lawyer-client relationship; and (vi) information about aggregate current and historical payment of fees (such as realization rates, average receivables, and aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

[18C] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily *not* permitted, however, if information is protected by Rule 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney-client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness in paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; or information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

[18D] When lawyers are exploring a new association, whether by lateral move or by merger, all lawyers involved must individually consider fiduciary obligations to their existing firms that may bear on the timing and scope of disclosures to clients relating to conflicts and financial concerns, and should consider whether to ask clients for a waiver of confidentiality if consistent with these fiduciary duties—*see* Rule 1.10(e) (requiring law firms to check for conflicts of interest). Questions of fiduciary duty are legal issues beyond the scope of the Rules.

[18E] For the unique confidentiality and notice provisions that apply to a lawyer or law firm seeking to sell all or part of its practice, see Rule 1.17 and Comment [7] to that Rule.

[18F] Before disclosing information regarding a possible lateral move or law firm merger, law firms and lawyers moving between firms—both those providing information and those receiving information—should use reasonable measures to minimize the risk of any improper, unauthorized or inadvertent disclosures, whether or not the information is protected by Rule 1.6(a), 1.9(c), or 1.18(b). These steps might include such measures as: (1) disclosing client information in stages; initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information outside the firm(s) during and after the lateral hiring negotiations or merger process.

RULE 5.1

RESPONSIBILITIES OF LAW FIRMS, PARTNERS, MANAGERS AND SUPERVISORY LAWYERS

(a) A law firm shall make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.

(b) (1) A lawyer with management responsibility in a law firm shall make reasonable efforts to ensure that other lawyers in the law firm conform to these Rules.

(2) A lawyer with direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the supervised lawyer conforms to these Rules.

(c) A law firm shall ensure that the work of partners and associates is adequately supervised, as appropriate. A lawyer with direct supervisory authority over another lawyer shall adequately supervise the work of the other lawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter, and the likelihood that ethical problems might arise in the course of working on the matter.

(d) A lawyer shall be responsible for a violation of these Rules by another lawyer if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the other lawyer practices or is a lawyer who has supervisory authority over the other lawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the con-

supervisory authority in particular circumstances is a question of fact. Partners and lawyers with comparable authority have at least indirect responsibility for all work being done by the firm, while a partner or manager in charge of a particular matter ordinarily also has supervisory responsibility for the work of other firm lawyers engaged in the matter. Partners and lawyers with comparable authority, as well as those who supervise other lawyers, are indirectly responsible for improper conduct of which they know or should have known in the exercise of reasonable managerial or supervisory authority. Appropriate remedial action by a partner or managing lawyer would depend on the immediacy of that lawyer's involvement and the seriousness of the misconduct. A supervisor is required to intervene to prevent misconduct or to prevent or mitigate avoidable consequences of misconduct if the supervisor knows that the misconduct occurred.

[6] Professional misconduct by a lawyer under supervision could reveal a violation of paragraph (a), (b) or (c) on the part of a law firm, partner or supervisory lawyer even though it does not entail a violation of paragraph (d) because there was no direction, ratification or knowledge of the violation or no violation occurred.

[7] Apart from this Rule and Rule 8.4(a), a lawyer does not have disciplinary liability for the conduct of another lawyer. Whether a lawyer may be liable civilly or criminally for another lawyer's conduct is a question of law beyond the scope of these Rules.

[8] The duties imposed by this Rule on managing and supervising lawyers do not alter the personal duty of each lawyer in a firm to abide by these Rules. *See* Rule 5.2(a).

RULE 5.2

RESPONSIBILITIES OF A SUBORDINATE LAWYER

(a) A lawyer is bound by these Rules notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate these Rules if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.

Comment

[1] Although a lawyer is not relieved of responsibility for a violation by the fact that the lawyer acted at the direction of a supervisor, that fact may be relevant in determining whether a lawyer had the knowledge required to render conduct a violation of these Rules. For example, if a subordinate filed a frivolous pleading at the direction of a supervisor, the subordinate would not be guilty of a professional violation unless the subordinate knew of the document's frivolous character.

[2] When lawyers in a supervisor-subordinate relationship encounter a matter involving professional judgment as to ethical duty, the supervisor may assume responsibility for making the judgment. Otherwise, a consistent course of action or position could not be taken. If the question can reasonably be answered only one way, the duty of both lawyers is clear, and they are equally responsible for fulfilling it. However, if the question is reasonably arguable, someone has to decide upon the course of action. That authority ordinarily reposes in the supervisor, and a subordinate may be guided accordingly. To evaluate the supervisor's conclusion that the question is arguable and the supervisor's resolution of it is reasonable in light of applicable Rules of Professional Conduct and other law, it is advisable that the subordinate lawyer undertake research, consult with a designated senior partner or special committee, if any (*see* Rule 5.1, Comment [3]), or use other appropriate means. For example, if a question arises whether the interests of two clients conflict under Rule 1.7, the supervisor's reasonable resolution of the question should protect the subordinate professionally if the resolution is subsequently challenged.

RULE 5.3

LAWYER'S RESPONSIBILITY FOR CONDUCT OF NONLAWYERS

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a lawyer who has supervisory authority over the nonlawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

Comment

[1] This Rule requires a law firm to ensure that work of nonlawyers is appropriately supervised. In addition, a lawyer with direct supervisory authority over the work of nonlawyers must adequately supervise

those nonlawyers. Comments [2] and [3] to Rule 5.1, which concern supervision of lawyers, provide guidance by analogy for the methods and extent of supervising nonlawyers.

[2] With regard to nonlawyers, who are not themselves subject to these Rules, the purpose of the supervision is to give reasonable assurance that the conduct of all nonlawyers employed by or retained by or associated with the law firm, including nonlawyers outside the firm working on firm matters, is compatible with the professional obligations of the lawyers and firm. Lawyers typically employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns and paraprofessionals. Such nonlawyer assistants, whether they are employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. Likewise, lawyers may employ nonlawyers outside the firm to assist in rendering those services. *See* Comment [6] to Rule 1.1 (retaining lawyers outside the firm). A law firm must ensure that such nonlawyer assistants are given appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose confidential information—*see* Rule 1.6 (c) (requiring lawyers to take reasonable care to avoid unauthorized disclosure of confidential information. Lawyers also should be responsible for the work done by their nonlawyer assistants. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline. A law firm should make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that nonlawyers in the firm and nonlawyers outside the firm who work on firm matters will act in a way compatible with the professional obligations of the lawyer. A lawyer with supervisory authority over a nonlawyer within or outside the firm has a parallel duty to provide appropriate supervision of the supervised nonlawyer.

[2A] Paragraph (b) specifies the circumstances in which a lawyer is responsible for conduct of a nonlawyer that would be a violation of these Rules if engaged in by a lawyer. For guidance by analogy, see Rule 5.1, Comments [5]-[8].

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include (i) retaining or contracting with an investigative or paraprofessional service, (ii) hiring a document management company to create and maintain a database for complex litigation, (iii) sending client documents to a third party for printing or scanning, and (iv) using an Internet-based service to

store client information. When using such services outside the firm, a lawyer or law firm must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of the reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the nonlawyer's work. *See also* Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4 (professional independence of the lawyer) and 5.5 (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

JUNE 2017

ABA Formal Opinion 477R: Securing communication of protected client information

Share:

Just this past week, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R (Revised May 22, 2017) on the subject of a lawyer's ethical obligations to protect confidential client information when transmitting information relating to the representation over the internet. The opinion takes a fresh look at advances in technology and ever-increasing cybersecurity threats, and provides guidance as to when enhanced security measures are appropriate.

This opinion is an update to ABA Formal Opinion 99-413 *Protecting the Confidentiality of Unencrypted E-Mail* (1999).

In 99-413, the committee concluded that since email provided a reasonable expectation of privacy, lawyers could use it to communicate with their clients, since it would be just as illegal to wiretap a telephone as it would be to intercept an email transmission. At the same time, the committee recognized that some information is so sensitive that a lawyer might consider using particularly strong protective measures depending on the sensitivity of the information:

> ... The conclusions reached in this opinion do not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of

> highly sensitive matters. Those measures might include the avoidance of email, just as they would warrant the avoidance of the telephone, fax and mail. – Formal Opinion 99-413 at page 2.

Since the time of Opinion 99-413, times have changed especially in the realm of technology and its many new and evolving manifestations that have become widespread in the profession. Laptop computers, smartphones, social media, cloud storage and Wi-Fi connections have become prevalent and much more commonplace than they were when 99-413 was written nearly 18 years ago.

The ABA Model Rules of Professional Conduct have also undergone several changes, particularly those that focus on a lawyer's obligation to protect client confidences when transmitting information over the internet.

Chief among these were the amendments to Rule 1.1 *Competence* and 1.6 *Confidentiality of Information* of the ABA Model Rules of Professional Conduct that were proposed by the ABA Ethics 20/20 Commission and subsequently adopted by the ABA House of Delegates at the 2012 ABA Annual Meeting. (The Ethics 20/20 Commission's Report and Recommendation concerning these amendments is available here.)

Paragraph 8 of the Comment to Rule 1.1 now states that "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology…*"

The commission also added a new subpart (c) to Rule 1.6 that states:

> **A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.**

Paragraph 18 of the Comment to Rule 1.6 was also amended, making it clear that additional methods of security should be considered depending upon the sensitivity of the information that is to be transmitted.

In Opinion 477R, the committee took note of the increasing sophistication of cyber threats in today's technological environment and recognized that some new forms of electronic communication that have become commonplace may not in every instance provide a reasonable expectation of privacy:

> ...In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.
>
> However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable - Formal Opinion 477R at p. 5

In order to determine when additional security methods are required, the committee turned to the factors outlined in paragraph 18 of the Comment to Model Rule 1.6:

- The sensitivity of the information
- The likelihood of disclosure if additional safeguards are not employed

- The cost of employing additional safeguards
- The difficulty of implementing the safeguards and
- The extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

The committee recommended the following steps lawyers should take to guard against disclosures, including:

1. Understand the nature of the threat. Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.

2. Understand how client confidential information is transmitted and where it is stored. Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.

3. Understand and use reasonable electronic security measures. Have an understanding of the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.

4. Determine how electronic communications about clients' matters should be protected. Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.

5. Label client confidential information. Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.

6. Train lawyers and nonlawyer assistants in technology and information security. Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.

7. Conduct due diligence on vendors providing communication technology. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.

TOPIC:

ETHICS

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com (explaining that "[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence."); *See also Criminal-Seeking-Hacker' Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,[6] and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.[7]

[6] The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

[7] In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g.*, *Cybersecurity Resources*, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[8] The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[9]

In recommending the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to 'keep abreast of changes in the law and its practice.' The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [10]

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[10] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[11]

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).

[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").

[14] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF'L CONDUCT R. 1.15 (2018).

[15] *See also* MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2018).

[16] The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); *See also* National Cyber Security Centre "Ten Steps to Cyber Security" [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.[18] The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. "One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents."[19] While every lawyer's response plan should be tailored to the lawyer's or the law firm's specific practice, as a general matter incident response plans share common features:

> The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

[18] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting "an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.").

[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.[20]

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[21] These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).
[21] We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).[22] Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[23] The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[24]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

[22] The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

[24] *Id.* at (c).

- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[25]

As this Committee recognized in ABA Formal Opinion 477R:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.[26] Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.[27] As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[28]

[25] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2018). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

[26] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

[27] MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. [18] (2018) ("The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.")

[28] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.[29] In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.[30] We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.[31]

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[30] This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

[31] Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: "If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach."[32] The Committee advised:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).[33]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.[34]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[33] *Id.*

[34] MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property." Funds must be kept in a separate account, and "[o]ther property shall be identified as such and appropriately safeguarded." Model Rule 1.15(a) also provides that, "Complete records of such account funds and other property shall be kept by the lawyer . . . ." Comment [1] to Model Rule 1.15 states:

> A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form. Comment [1] uses as examples "securities" and "property" that should be kept separate from the lawyer's "business and personal property." That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15's safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, "Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information."

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client."[35] When electronic "information relating to the representation" of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the former client. Rule 1.9(c) provides that a lawyer "shall not . . . reveal" the former client's information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] We also note that Rule 1.16(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.[38] Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).
[36] *See* Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent's argument that the court should engraft an additional element of proof in a disciplinary charge because "such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.").
[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).
[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.[39]

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

[39] *Cf.* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.[40] Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

[40] State Bar of Mich. Op. RI-09 (1991).

[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[42] *Id.*

[43] *Id.*

[44] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.

[45] Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients “reasonably informed” and with an explanation “to the extent necessary to permit the client to make informed decisions regarding the representation.”

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328
CHAIR: Barbara S. Gillers, New York, NY ■ John M. Barkett, Miami, FL ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Michael H. Rubin, Baton Rouge, LA ■ Lynda Shely, Scottsdale, AZ ■ Elizabeth C. Tarbert, Tallahassee, FL. ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 498 **March 10, 2021**

Virtual Practice

The ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm.[1] *When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.*

I. Introduction

As lawyers increasingly use technology to practice virtually, they must remain cognizant of their ethical responsibilities. While the ABA Model Rules of Professional Conduct permit virtual practice, the Rules provide some minimum requirements and some of the Comments suggest best practices for virtual practice, particularly in the areas of competence, confidentiality, and supervision. These requirements and best practices are discussed in this opinion, although this opinion does not address every ethical issue arising in the virtual practice context.[2]

II. Virtual Practice: Commonly Implicated Model Rules

This opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional brick-and-mortar law firm.[3] A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] Interstate virtual practice, for instance, also implicates Model Rule of Professional Conduct 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law, which is not addressed by this opinion. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 495 (2020), stating that "[l]awyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction."

[3] *See generally* MODEL RULES OF PROFESSIONAL CONDUCT R. 1.0(c), defining a "firm" or "law firm" to be "a lawyer or lawyers in a partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization on the legal department of a corporation or other organization." Further guidance on what constitutes a firm is provided in Comments [2], [3], and [4] to Rule 1.0.

have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need. Although the ethics rules apply to both traditional and virtual law practice,[4] virtual practice commonly implicates the key ethics rules discussed below.

A. *Commonly Implicated Model Rules of Professional Conduct*

1. Competence, Diligence, and Communication

Model Rules 1.1, 1.3, and 1.4 address lawyers' core ethical duties of competence, diligence, and communication with their clients. Comment [8] to Model Rule 1.1 explains, "To maintain the requisite knowledge and skill [to be competent], a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology,* engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (*Emphasis added*). Comment [1] to Rule 1.3 makes clear that lawyers must also "pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor." Whether interacting face-to-face or through technology, lawyers must "reasonably consult with the client about the means by which the client's objectives are to be accomplished; . . . keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information. . . ."[5] Thus, lawyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually.[6]

2. Confidentiality

Under Rule 1.6 lawyers also have a duty of confidentiality to all clients and therefore "shall not reveal information relating to the representation of a client" (absent a specific exception, informed consent, or implied authorization). A necessary corollary of this duty is that lawyers must at least "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[7] The following non-

[4] For example, if a jurisdiction prohibits substantive communications with certain witnesses during court-related proceedings, a lawyer may not engage in such communications either face-to-face or virtually (e.g., during a trial or deposition conducted via videoconferencing). *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 3.4(c) (prohibiting lawyers from violating court rules and making no exception to the rule for virtual proceedings). Likewise, lying or stealing is no more appropriate online than it is face-to-face. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.15; MODEL RULES OF PROF'L CONDUCT R. 8.4(b)-(c).

[5] MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(2) – (4).

[6] Lawyers unexpectedly thrust into practicing virtually must have a business continuation plan to keep clients apprised of their matters and to keep moving those matters forward competently and diligently. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) (discussing ethical obligations related to disasters). Though virtual practice is common, if for any reason a lawyer cannot fulfill the lawyer's duties of competence, diligence, and other ethical duties to a client, the lawyer must withdraw from the matter. MODEL RULES OF PROF'L CONDUCT R. 1.16. During and following the termination or withdrawal process, the "lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred." MODEL RULES OF PROF'L CONDUCT R. 1.16(d).

[7] MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

exhaustive list of factors may guide the lawyer's determination of reasonable efforts to safeguard confidential information: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[8] As ABA Formal Op. 477R notes, lawyers must employ a "fact-based analysis" to these "nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."

Similarly, lawyers must take reasonable precautions when transmitting communications that contain information related to a client's representation.[9] At all times, but especially when practicing virtually, lawyers must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information. This responsibility "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[10] However, depending on the circumstances, lawyers may need to take special precautions.[11] Factors to consider to assist the lawyer in determining the reasonableness of the "expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."[12] As ABA Formal Op. 477R summarizes, "[a] lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."

3. Supervision

Lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct.[13] Practicing virtually does not change or diminish this obligation. "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."[14] Moreover, a lawyer must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent

[8] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18].

[9] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].

[10] *Id.*

[11] The opinion cautions, however, that "a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

[12] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].

[13] MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3. *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 467 (2014) (discussing managerial and supervisory obligations in the context of prosecutorial offices). *See also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 n.6 (2018) (describing the organizational structures of firms as pertaining to supervision).

[14] MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [2].

or unauthorized disclosure by the lawyer *or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision*."[15] The duty to supervise nonlawyers extends to those both within and outside of the law firm.[16]

B. Particular Virtual Practice Technologies and Considerations

Guided by the rules highlighted above, lawyers practicing virtually need to assess whether their technology, other assistance, and work environment are consistent with their ethical obligations. In light of current technological options, certain available protections and considerations apply to a wide array of devices and services. As ABA Formal Op. 477R noted, a "lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software." Furthermore, "[o]ther available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems." To apply and expand on these protections and considerations, we address some common virtual practice issues below.

1. Hard/Software Systems

Lawyers should ensure that they have carefully reviewed the terms of service applicable to their hardware devices and software systems to assess whether confidentiality is protected.[17] To protect confidential information from unauthorized access, lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs). Finally, as technology inevitably evolves, lawyers should periodically assess whether their existing systems are adequate to protect confidential information.

[15] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (emphasis added).

[16] As noted in Comment [3] to Model Rule 5.3:

> When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law).

[17] For example, terms and conditions of service may include provisions for data-soaking software systems that collect, track, and use information. Such systems might purport to own the information, reserve the right to sell or transfer the information to third parties, or otherwise use the information contrary to lawyers' duty of confidentiality.

2. Accessing Client Files and Data

Lawyers practicing virtually (even on short notice) must have reliable access to client contact information and client records. If the access to such "files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer."[18] Lawyers must ensure that data is regularly backed up and that secure access to the backup data is readily available in the event of a data loss. In anticipation of data being lost or hacked, lawyers should have a data breach policy and a plan to communicate losses or breaches to the impacted clients.[19]

3. Virtual meeting platforms and videoconferencing

Lawyers should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer's ethical obligations. Access to accounts and meetings should be only through strong passwords, and the lawyer should explore whether the platform offers higher tiers of security for businesses/enterprises (over the free or consumer platform variants). Likewise, any recordings or transcripts should be secured. If the platform will be recording conversations with the client, it is inadvisable to do so without client consent, but lawyers should consult the professional conduct rules, ethics opinions, and laws of the applicable jurisdiction.[20] Lastly, any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by other third parties who are not assisting with the representation,[21] to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality.

4. Virtual Document and Data Exchange Platforms

In addition to the protocols noted above (e.g., reviewing the terms of service and any updates to those terms), lawyers' virtual document and data exchange platforms should ensure that

[18] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018).

[19] *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) ("Even lawyers who, (i) under Model Rule 1.6(c), make 'reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,' (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'").

[20] *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-422 (2001).

[21] Pennsylvania recently highlighted the following best practices for videoconferencing security:

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to "Host Only;"
- Ensure users are using the updated version of remote access/meeting applications.

Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2020-300 (2020) (citing an FBI press release warning of teleconference and online classroom hacking).

documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure. For example, if the lawyer is transmitting information over email, the lawyer should consider whether the information is and needs to be encrypted (both in transit and in storage).[22]

5. Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices

Unless the technology is assisting the lawyer's law practice, the lawyer should disable the listening capability of devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters. Otherwise, the lawyer is exposing the client's and other sensitive information to unnecessary and unauthorized third parties and increasing the risk of hacking.

6. Supervision

The virtually practicing managerial lawyer must adopt and tailor policies and practices to ensure that all members of the firm and any internal or external assistants operate in accordance with the lawyer's ethical obligations of supervision.[23] Comment [2] to Model Rule 5.1 notes that "[s]uch policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

a. Subordinates/Assistants

The lawyer must ensure that law firm tasks are being completed in a timely, competent, and secure manner.[24] This duty requires regular interaction and communication with, for example,

[22] *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) (noting that "it is not always reasonable to rely on the use of unencrypted email").

[23] As ABA Formal Op. 477R noted:

> In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

[24] The New York County Lawyers Association Ethics Committee recently described some aspects to include in the firm's practices and policies:

- Monitoring appropriate use of firm networks for work purposes.
- Tightening off-site work procedures to ensure that the increase in worksites does not similarly increase the entry points for a data breach.
- Monitoring adherence to firm cybersecurity procedures (e.g., not processing or transmitting work across insecure networks, and appropriate storage of client data and work product).
- Ensuring that working at home has not significantly increased the likelihood of an inadvertent disclosure through misdirection of a transmission, possibly because the lawyer or nonlawyer was distracted by a child, spouse, parent or someone working on repair or maintenance of the home.

associates, legal assistants, and paralegals. Routine communication and other interaction are also advisable to discern the health and wellness of the lawyer's team members.[25]

One particularly important subject to supervise is the firm's bring-your-own-device (BYOD) policy. If lawyers or nonlawyer assistants will be using their own devices to access, transmit, or store client-related information, the policy must ensure that security is tight (e.g., strong passwords to the device and to any routers, access through VPN, updates installed, training on phishing attempts), that any lost or stolen device may be remotely wiped, that client-related information cannot be accessed by, for example, staff members' family or others, and that client-related information will be adequately and safely archived and available for later retrieval.[26]

Similarly, all client-related information, such as files or documents, must not be visible to others by, for example, implementing a "clean desk" (and "clean screen") policy to secure documents and data when not in use. As noted above in the discussion of videoconferencing, client-related information also should not be visible or audible to others when the lawyer or nonlawyer is on a videoconference or call. In sum, all law firm employees and lawyers who have access to client information must receive appropriate oversight and training on the ethical obligations to maintain the confidentiality of such information, including when working virtually.

b. Vendors and Other Assistance

Lawyers will understandably want and may need to rely on information technology professionals, outside support staff (e.g., administrative assistants, paralegals, investigators), and vendors. The lawyer must ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties. When appropriate, lawyers should consider use of a confidentiality agreement,[27] and should ensure that all client-related information is secure, indexed, and readily retrievable.

7. Possible Limitations of Virtual Practice

Virtual practice and technology have limits. For example, lawyers practicing virtually must make sure that trust accounting rules, which vary significantly across states, are followed.[28] The

- Ensuring that sufficiently frequent "live" remote sessions occur between supervising attorneys and supervised attorneys to achieve effective supervision as described in [New York Rule of Professional Conduct] 5.1(c).

N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 754-2020 (2020).

[25] *See* ABA MODEL REGULATORY OBJECTIVES FOR THE PROVISION OF LEGAL SERVICES para. I (2016).

[26] For example, a lawyer has an obligation to return the client's file when the client requests or when the representation ends. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.16(d). This important obligation cannot be fully discharged if important documents and data are located in staff members' personal computers or houses and are not indexed or readily retrievable by the lawyer.

[27] *See, e.g.*, Mo. Bar Informal Advisory Op. 20070008 & 20050068.

[28] *See* MODEL RULES OF PROF'L CONDUCT R. 1.15; *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) ("Lawyers also must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust. A lawyer's obligations with respect to these funds will vary depending on the circumstances. Even before a disaster, all lawyers should consider (i) providing for another trusted signatory on trust

lawyer must still be able, to the extent the circumstances require, to write and deposit checks, make electronic transfers, and maintain full trust-accounting records while practicing virtually. Likewise, even in otherwise virtual practices, lawyers still need to make and maintain a plan to process the paper mail, to docket correspondence and communications, and to direct or redirect clients, prospective clients, or other important individuals who might attempt to contact the lawyer at the lawyer's current or previous brick-and-mortar office. If a lawyer will not be available at a physical office address, there should be signage (and/or online instructions) that the lawyer is available by appointment only and/or that the posted address is for mail deliveries only. Finally, although e-filing systems have lessened this concern, litigators must still be able to file and receive pleadings and other court documents.

III. Conclusion

The ABA Model Rules of Professional Conduct permit lawyers to conduct practice virtually, but those doing so must fully consider and comply with their applicable ethical responsibilities, including technological competence, diligence, communication, confidentiality, and supervision.

accounts in the event of the lawyer's unexpected death, incapacity, or prolonged unavailability and (ii) depending on the circumstances and jurisdiction, designating a successor lawyer to wind up the lawyer's practice.").

NEW YORK STATE BAR ASSOCIATION

NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

New York State Bar Association
Committee on Professional Ethics

Opinion 1240 (04/08/2022)

Topic: Duty to protect client information stored on a lawyer's smartphone.

Digest: If "contacts" on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent.

Rules: 1.6

FACTS:

1. When the inquiring lawyer downloads or accesses an app on his smartphone, the lawyer is sometimes asked whether the lawyer gives consent for that app to access the lawyer's "contacts" on the smartphone. The lawyer's contacts include clients in criminal representations.

QUESTION:

2. May a lawyer consent for an app to access contacts on the lawyer's smartphone that include the lawyer's current, former or prospective clients?

OPINION:

3. Rule 1.6(c) of the New York Rules of Professional Conduct (the "Rules") requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to" the confidential information of current, former and prospective clients. Rule 1.6(a), in turn, provides that confidential information "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

4. Rule 1.6(c) has been interpreted to require a lawyer to take reasonable care to protect clients' confidential information when carrying electronic devices containing such information across the border (see N.Y. City 2017-5 (2017)), when using an online storage provider to store clients' confidential information (see N.Y. State 842 (2010)), and when sending emails containing confidential information (see N.Y. State 709 (1998)).

5. In N.Y. State 820 (2008), we applied this general principle to a lawyer's use of an e-mail service provider that scans e-mails for keywords and sends or displays targeted computer-generated advertisements to the lawyer using the service based on the words in the e-mail communications. We concluded that using such a service is permissible if "[u]nder the particular e-mail provider's published privacy policies, no individuals other than e-mail senders and recipients read the e-mail messages, are otherwise privy to their content or receive targeted advertisements from the service provider." We reasoned: "Merely scanning the content of e-mails by computer to generate computer advertising . . . does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the emails' content." In contrast, we stated it would not be permissible to use the service "if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order)." Accordingly, we opined that a "lawyer must exercise due care in selecting an e-mail service provider to ensure that its policies and stated practices protect client confidentiality" in conformance with these governing principles.

6. In N.Y. State 1088 (2016), we addressed whether an attorney could disclose to a potential client the names of actual clients the attorney had represented in the same practice area. To answer that inquiry, we needed to determine, as a threshold matter, whether and under what circumstances the names of current or past clients could be "confidential information," as defined in Rule 1.6(a). We stated, first, that clients' names will be confidential information if the clients have requested keeping their names confidential. See N.Y. State 1088 ¶ 6 (2016). We then opined:

> If the client has not requested that the lawyer keep the client's name confidential, then the lawyer must determine whether the fact of representation is generally known and, if not, whether disclosing the identity of the client and the fact of representation is likely to be embarrassing or detrimental to the client. This will depend on the client and the specific facts and circumstances of the representation.

N.Y. State 1088 ¶ 7.

7. We discussed in Opinion 1088 what it meant to be "generally known" within the meaning of Rule 1.6(a) (¶ 8) and stated, "The client is more likely to find that disclosure of the fact of a current or prior representation by a lawyer is embarrassing or detrimental where the representation involves or involved criminal law, bankruptcy, debt collection or family law." Id. ¶ 9. Finally, we noted there might be other factors, other than the subject matter of the representation, that are relevant to determine whether the client would object to being identified as the lawyer's client. Id. ¶ 10.

8. Contacts stored on a smartphone typically include one or more email addresses, work or residence addresses, and phone numbers (collectively sometimes called "directory information"), but contacts often also include additional non-directory information (such as birth date or the lawyer's relationship to the contact). Social media apps may seek access to this information to solicit more users to the platform or to establish links between users and enhance the user experience. Apps which sell products or services may seek such access to promote additional sales. Apps that espouse political or social beliefs may seek such access to disseminate their views. These are but three examples of how an attorney's contacts might be exploited by an app, but there are more, and likely many more to come.

9. Insofar as clients' names constitute confidential information, a lawyer must make reasonable efforts to prevent the unauthorized access of others to those names, whether stored as a paper copy in a filing cabinet, on a smartphone, or in any other electronic or paper form. To that end, before an attorney grants access to the attorney's contacts, the attorney must determine whether any contact – even one – is confidential within the meaning of Rule 1.6(a). A contact could be confidential because it reflects the existence of a client-attorney relationship which the client requested not be disclosed or which, based upon particular facts and circumstances, would be likely to be embarrassing or detrimental to the client if disclosed. N.Y. State 1088 (2016).

10. Some relevant factors a lawyer should consider in determining whether any contacts are confidential are: (i) whether the contact information identifies the smartphone owner as an attorney, or more specifically identifies the attorney's area of practice (such as criminal law, bankruptcy law, debt collection law, or family law); (ii) whether people included in the contacts are identified as clients, as friends, as something else, or as nothing at all; and (iii) whether the contact information also includes email addresses, residence addresses, telephone numbers, names of family members or business associates, financial data, or other personal or non-public information that is not generally known.

11. If a lawyer determines that the contacts stored on his smartphone include the confidential information of any current or former client, the lawyer must not consent to give access to his contacts to an app, unless the attorney, after reasonable due diligence, including a review of the app's policies and stated practices to protect user information and user privacy, concludes that such confidential contact information will be handled in such a manner and for such limited purposes that it will not, absent the client's consent, be disclosed to additional third party persons, systems or entities. See N.Y. State 820 (2008).

CONCLUSION:

12. If "contacts" on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent.

(34-21)

NYSBA NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, New York 12207 □ PH 518.463.3200 □ www.nysba.org

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, *e.g.:*

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102(D) [now Rule 1.15(d)].
N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.
N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".
N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.
N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.
N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.
N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.
N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not

knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also noted, however, that "when the confidential information is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted internet e-mail." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving the use of "cloud" data storage, we were told that the storage system was password protected and that data stored in the system was encrypted. We concluded that the lawyer could

use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

> (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
>
> (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
>
> (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
>
> (4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, Locked Down: Information Security for Lawyers (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j).

7-14

NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. May a lawyer use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty? If so, what steps should the lawyer take to ensure that the information is sufficiently secure?

OPINION

2. Various companies offer online computer data storage systems that are maintained on an array of Internet servers located around the world. (The array of Internet servers that store the data is often called the "cloud.") A solo practitioner would like to use one of these online "cloud" computer data storage systems to store client confidential information. The lawyer's aim is to ensure that his clients' information will not be lost if something happens to the lawyer's own computers. The online data storage system is password-protected and the data stored in the online system is encrypted.

3. A discussion of confidential information implicates Rule 1.6 of the New York Rules of Professional Conduct (the “Rules”), the general rule governing confidentiality. Rule 1.6(a) provides as follows:

> A lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of a lawyer or a third person, unless:
>
> (1) the client gives informed consent, as defined in Rule 1.0(j);
>
> (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
>
> (3) the disclosure is permitted by paragraph (b).

4. The obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client’s confidential information. *See* N.Y. County 733 (2004) (an attorney “must diligently preserve the client’s confidences, whether reduced to digital format, paper, or otherwise”). As a New Jersey ethics committee observed, even when a lawyer wants a closed client file to be destroyed, "[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties." New Jersey Opinion (2006), *quoting* New Jersey Opinion 692 (2002).

5. In addition, Rule 1.6(c) provides that an attorney must “exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client” except to the extent disclosure is permitted by Rule 1.6(b). Accordingly, a lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney’s supervision or who have been retained by the attorney to assist in providing services to the client. We note, however, that exercising "reasonable care" under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access.

6. To date, no New York ethics opinion has addressed the ethics of *storing* confidential information online. However, in N.Y. State 709 (1998) this Committee addressed the duty to preserve a client’s confidential information when *transmitting* such information electronically. Opinion 709 concluded that lawyers may transmit confidential information by e-mail, but cautioned that “lawyers must always act reasonably in choosing to use e-mail for confidential communications.” The Committee also warned that the exercise of reasonable care may differ from one case to the next. Accordingly, when a lawyer is on notice that the confidential information being transmitted is “of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer’s control, the lawyer

must select a more secure means of communication than unencrypted Internet e-mail." *See also* Rule 1.6, cmt. 17 (a lawyer "must take reasonable precautions" to prevent information coming into the hands of unintended recipients when transmitting information relating to the representation, but is not required to use special security measures if the means of communicating provides a reasonable expectation of privacy).

7. Ethics advisory opinions in several other states have approved the use of electronic storage of client files provided that sufficient precautions are in place. *See, e.g.*, New Jersey Opinion 701 (2006) (lawyer may use electronic filing system whereby all documents are scanned into a digitized format and entrusted to someone outside the firm provided that the lawyer exercises "reasonable care," which includes entrusting documents to a third party with an enforceable obligation to preserve confidentiality and security, and employing available technology to guard against reasonably foreseeable attempts to infiltrate data); Arizona Opinion 05-04 (2005) (electronic storage of client files is permissible provided lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence"); *see also* Arizona Opinion 09-04 (2009) (lawyer may provide clients with an online file storage and retrieval system that clients may access, provided lawyer takes reasonable precautions to protect security and confidentiality and lawyer periodically reviews security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected).

8. Because the inquiring lawyer will use the online data storage system for the purpose of preserving client information - a purpose both related to the retention and necessary to providing legal services to the client - using the online system is consistent with conduct that this Committee has deemed ethically permissible. *See* N.Y. State 473 (1977) (absent client's objection, lawyer may provide confidential information to outside service agency for legitimate purposes relating to the representation provided that the lawyer exercises care in the selection of the agency and cautions the agency to keep the information confidential); *cf.* NY CPLR 4548 (privileged communication does not lose its privileged character solely because it is communicated by electronic means or because "persons necessary for the delivery or facilitation of such electronic communication may have access to" its contents).

9. We conclude that a lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. *See* Rule 1.4 (mandating communication with clients); *see also* N.Y. State 820 (2008) (addressing Web-based email services).

11. Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *See, e.g.*, *City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619, 177 L.Ed.2d 216 (2010) (holding that City did not violate Fourth Amendment when it reviewed transcripts of messages sent and received by police officers on police department pagers); *Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. 2007) (e-mails between hospital employee and his personal attorneys were not privileged because employer's policy regarding computer use and e-mail monitoring stated that employees had no reasonable expectation of privacy in e-mails sent over the employer's e-mail server). *But see Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 990 A.2d 650 (2010) (despite employer's e-mail policy stating that company had right to review and disclose all information on "the company's media systems and services" and that e-mails were "not to be considered private or personal" to any employees, company violated employee's attorney-client privilege by reviewing e-mails sent to employee's personal attorney on employer's laptop through employee's personal, password-protected e-mail account).

12. This Committee's prior opinions have addressed the disclosure of confidential information in metadata and the perils of practicing law over the Internet. We have noted in those opinions that the duty to "exercise reasonable care" to prevent disclosure of confidential information "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks" in transmitting information electronically. N.Y. State 782 (2004), *citing* N.Y. State 709 (1998) (when conducting trademark practice over the Internet, lawyer had duty to "stay abreast of this evolving

technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost"); *see also* N.Y. State 820 (2008) (same in context of using e-mail service provider that scans e-mails to generate computer advertising). The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.

CONCLUSION

13. A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.

(75-09)

Cybersecurity, Privacy and Data Protection FAQs

The following Frequently Asked Questions (FAQs) relate to the changes in the New York State CLE Program Rules and the New York State CLE Board Regulations and Guidelines adding Cybersecurity, Privacy and Data Protection as a new CLE category of credit (effective January 1, 2023) and requiring that attorneys complete at least 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their biennial CLE requirement (effective July 1, 2023).

Experienced Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] Experienced attorneys (admitted to the New York Bar for more than two years) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their biennial CLE requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics.**

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that experienced attorneys must complete during each biennial reporting cycle?

A] No, experienced attorneys must still earn at least 24 CLE credit hours each biennial reporting cycle as follows:

Experienced Attorney Required CLE Categories **(for attorneys due to re-register on or after July 1, 2023)**	**Required CLE Credit Hours**
Ethics and Professionalism	4
Diversity, Inclusion and Elimination of Bias	1
Cybersecurity, Privacy and Data Protection (General or Ethics)	1*
Any CLE category of credit	18
Total Number of CLE credit hours	**24**

*You may choose to complete the Cybersecurity credit in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics**).

You may count a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 4-credit Ethics and Professionalism requirement.

- *Example*: if you earn 3 credits in Cybersecurity Ethics, then you still need to earn 1 credit in Ethics and Professionalism, 1 credit in Diversity, Inclusion and Elimination of Bias and 19 credits in any category of credit -- total of 24 credits

Q] When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] The new requirement becomes effective July 1, 2023.

- If you are **due to re-register on or after July 1, 2023 (birthday is on or after July 1st)**, you must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of your biennial CLE requirement.
- If you are **due to re-register in 2023 but your birthday is before July 1st**, you need **not** comply with the new requirement in 2023, but must comply in future biennial periods.
  - Example: If your birthday is on June 30th and you are due to re-register in 2023, then you do not need to comply with the new requirement in 2023, even if you file your registration form on or after July 1, 2023.
- If you are due to re-register in 2024, or later, you must comply with the new requirement.

Q] I'm due to re-register on or after July 1, 2023, but I won't be able to complete the Cybersecurity, Privacy and Data Protection requirement on time. What should I do?

A] You may apply for an extension of time to complete the CLE requirement.

Q] If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] May I satisfy any of my Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?

A] Yes, you may satisfy a maximum of 3 credits of your Ethics and Professionalism requirement with the same number of Cybersecurity, Privacy and Data Protection-Ethics credits.

Q] May I carry over Cybersecurity, Privacy and Data Protection CLE credits from one biennial reporting cycle to the next?

A] Yes. Once you have completed the 24-CLE credit requirement, a maximum of 6 additional credits earned may be applied toward the next reporting cycle. Experienced attorneys may carry over credits in any category, including Cybersecurity, Privacy and Data Protection, from one cycle to the next.

Newly Admitted Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] Newly admitted attorneys (admitted to the New York Bar for two years or less) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their newly admitted cycle requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics.**

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that newly admitted attorneys must complete during the newly admitted cycle?

A] No, newly admitted attorneys must still earn a total of 32 CLE credit hours (with 16 credit hours each year) in the newly admitted cycle as follows:

Newly Admitted Attorney Required CLE Categories (for attorneys admitted on or after July 1, 2023)	**Year 1 CLE Credit Hours**	**Year 2 CLE Credit Hours**
Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection-**General**	7 see below	7 see below
Skills	6	6
Ethics and Professionalism	3	3
Cybersecurity, Privacy and Data Protection-**Ethics**	see below	see below
Total Number of CLE credit hours	**16**	**16**

Cybersecurity, Privacy and Data Protection ("Cybersecurity") Category

- You must complete at least 1 credit in Cybersecurity as part of the 32-credit requirement.
- You may choose to complete the Cybersecurity credit:
  - in Year 1 or Year 2 (as part of the 16 credit-requirement for that year)
  - in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two)
- You may apply a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 6-credit Ethics and Professionalism requirement
  - *Example*: if you complete 1 credit in Cybersecurity **Ethics** in Year 1, you satisfy your Cybersecurity requirement, and then need to complete only 2 credits in Ethics and Professionalism for that year.
  - *Example*: if you complete 1 credit in Cybersecurity **General** in Year 1, you satisfy your Cybersecurity requirement and must complete an additional 6 credits in Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection-**General** for that year.

Q] **When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?**

A] The new requirement becomes effective July 1, 2023 for attorneys **admitted to the NY Bar on or after** July 1, 2023.

- If you were admitted to the NY Bar **prior to July 1, 2023**, you need not comply with the Cybersecurity, Privacy and Data Protection requirement in your newly admitted cycle, but must comply in future reporting cycles.
- Attorneys admitted to the NY Bar **on or after July 1, 2023**, must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their newly admitted attorney CLE requirement.

Q] **When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?**

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] **If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?**

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] **Do I need to complete the Cybersecurity, Privacy and Data Protection CLE requirement in <u>each</u> year of my newly admitted cycle, i.e., 1 Cybersecurity CLE credit in Year 1 and 1 Cybersecurity CLE credit in Year 2?**

A] No, you only need to complete 1 CLE credit in Cybersecurity, Privacy and Data Protection during your newly admitted cycle.

Q] **Do I need to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement during the first or second year of my newly admitted cycle?**

A] You can choose to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement in the first or second year of your newly admitted cycle as part of your 16-credit requirement for the year.

Q] **May I carry over Cybersecurity, Privacy and Data Protection CLE credits?**

A] Credit in Cybersecurity, Privacy and Data Protection-**Ethics** may **<u>not</u>** be carried over. Credit in Cybersecurity, Privacy and Data Protection-**General** **<u>may</u>** be carried over. For more information on carryover credit, please read the Newly Admitted FAQs.

Q] Do Cybersecurity, Privacy and Data Protection credits count toward my Ethics and Professionalism requirement?

A] You may count a maximum of 3 Cybersecurity, Privacy and Data Protection-**Ethics** credits toward your Ethics and Professionalism requirement in your newly admitted cycle. Cybersecurity, Privacy and Data Protection-**General** credits **do not** count toward your Ethics and Professionalism requirement.

Q] May I satisfy my entire Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?

A] No, you may satisfy a maximum of 3 credits of your total 6-credit Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-**Ethics** courses. By doing so, you would also satisfy your 1-credit Cybersecurity requirement.

Q] As a newly admitted attorney, in what formats can I take Cybersecurity, Privacy and Data Protection courses?

A] For Cybersecurity, Privacy and Data Protection-**General** courses, you may earn CLE credit in **any** approved format, including on-demand audio/video or webconference. For Cybersecurity, Privacy and Data Protection-**Ethics** courses, you may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Provider FAQs

Q] What may be addressed in Cybersecurity, Privacy and Data Protection programs?

A] Cybersecurity, Privacy and Data Protection CLE programs must relate to the practice of law, be specifically tailored to a legal audience, and aim to increase attorneys' professional ***legal*** competency. Please read Guidance for CLE Providers relating to Cybersecurity **Ethics** program areas and Cybersecurity **General** program areas.

Q] When may we begin to issue CLE credit in Cybersecurity, Privacy and Data Protection?

A] Providers may begin to issue credit in Cybersecurity, Privacy and Data Protection as of January 1, 2023, to attorneys who complete courses in this new category on or after January 1, 2023.

Q] What are the permissible formats for Cybersecurity, Privacy and Data Protection courses?

A] Experienced Attorneys: for Cybersecurity, Privacy and Data Protection (Ethics and General) courses, experienced attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.

Newly Admitted Attorneys:

- for Cybersecurity **General** courses, newly admitted attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.
- for Cybersecurity **Ethics** courses, newly admitted attorneys may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Q] We offered a live cybersecurity training in 2022 or earlier; can we issue CLE credit in the Cybersecurity, Privacy and Data Protection category to the attendees of this training?

A] No, you may not issue CLE credit in Cybersecurity, Privacy and Data Protection to the attendees of live courses that occurred prior to January 1, 2023.

Q] May we issue revised certificates awarding credit in the new Cybersecurity, Privacy and Data Protection category to attorneys who completed cybersecurity training in 2022 or earlier?

A] No. You may not issue revised certificates of attendance awarding credit in Cybersecurity, Privacy and Data Protection for courses completed prior to January 1, 2023.

Q] We issued CLE credit in Law Practice Management and Ethics and Professionalism for a course on cybersecurity in 2022 and we recorded the training. Can we issue CLE credit in the Cybersecurity, Privacy and Data Protection CLE category to participants who complete the prerecorded program on or after January 1, 2023?

A] Yes, assuming the content of the prerecorded program is timely and falls within the definition of Cybersecurity, Privacy and Data Protection, you can issue credit in Cybersecurity, Privacy and Data Protection to attorneys who complete the prerecorded program on or after January 1, 2023. Please note -- for newly admitted attorneys, the prerecorded format is permissible for credit in Cybersecurity, Privacy and Data Protection-**General** but not for credit in Cybersecurity, Privacy and Data Protection-**Ethics**.

Q] Can we issue CLE credit in Cybersecurity, Privacy and Data Protection training where there is no attorney faculty member participating?

A] No. As with all CLE programs, the faculty for a Cybersecurity, Privacy and Data Protection program should include an attorney in good standing who must actively participate in the program.

Q] Will there be a revised New York CLE Certificate of Attendance?

A] Yes, a revised New York CLE Certificate of Attendance that includes Cybersecurity, Privacy and Data Protection will be available on the CLE website and must be used beginning on January 1, 2023.

NEW YORK STATE
ACADEMY OF TRIAL LAWYERS

PRESENTS:

"NAVIGATING THE LEGAL LANDSCAPE OF CYBERSECURITY"

ETHICS MONOGRAPH

BY:

MICHAEL S. ROSS, ESQ.
LAW OFFICES OF MICHAEL S. ROSS

August 20, 2024
1:00pm – 2:00pm

HOW CYBERSECURITY IS ETHICS-DRIVEN

The Ethical Principles

The Need For New York Lawyers To Be Cybersecurity Conscious Is Driven In Part By Bedrock Ethical Rules.

Rule 1.6 sets forth what information is confidential and sets forth the lawyer's obligations with respect to confidential information. And recall that what is "confidential" is far broader than what is privileged.

> "Rule 1.6 – CONFIDENTIALITY OF INFORMATION
>
> (a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:
>
> (1) the client gives informed consent, as defined in Rule 1.0(j);
>
> (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
>
> (3) the disclosure is permitted by paragraph (b).
>
> '*Confidential information' consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential.* Confidential information' does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to
> which the information relates.
>
> …
>
> (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c) [the former client rule], or 1.18(b) [the prospective client rule]." (Emphasis added.)

The unofficial New York State Bar Association "Comments" to Rule 1.6 make it clear that lawyers must adhere to their duties of "competence" (Rule 1.1) and "diligence" (Rule 1.3) in attempting to ensure that client confidences are protected by their legal and non-legal staff alike. Comments [16] through [17B] explain:

[16] Paragraph (c) is intended to protect confidential information. It imposes three related obligations: (i) preventing "inadvertent disclosure"; (ii) preventing "unauthorized disclosure"; and (iii) preventing "unauthorized access." Specifically, paragraph (c) of this Rule requires a lawyer to make reasonable efforts to safeguard confidential information against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client (or who are otherwise subject to the lawyer's supervision). Paragraph (c) also requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties. See also Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients.

[16A] Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18 does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to*: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule.* For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy confidentiality.

[17A] The prevalence of *hacking, phishing, spoofing, Internet scams, and other unauthorized digital intrusions* into electronic or digital means of communication and data storage used by lawyers underscores the need for lawyers and law firms to use reasonable and proportionate technology to safeguard information protected by Rules 1.6, 1.9, 1.11(c), or 1.18. *To protect such information, lawyers and law firms should use reasonable administrative, technical and physical safeguards that*

> *are proportionate to (a) the size, nature, and complexity of the practice, and (b) the sensitivity of the confidential information the practice maintains.*
>
> *[17B] A lawyer may also be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law* (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked Confidential or Confidential—Attorneys' Eyes Only; the Health Insurance Portability and Accountability Act of 1996 (HIPAA) may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. *The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.*" (Emphasis added.)

Key touchpoints which relate to the issue of lawyer responsibilities in connection with cybersecurity are:

1. A lawyer has a duty to make reasonable and proportionate efforts to protect confidential information from inadvertent or unauthorized disclosure.

2. That duty stems from the lawyer's duty, among other things, to be competent. As unofficial New York State Bar Association Comment [8] to Rule explains: "To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500."

3. The information a lawyer must take steps to protect is any information that is privileged, that the client explicitly requested be kept confidential, or *any information which, if disclosed, would be embarrassing or detrimental to the client.*

4. There are limited grounds for disclosing confidential information. None of those grounds covers hacking, or ransomware, or phishing, or negligent or inadvertent disclosure to a third party.

There is, however, a related issue concerning cybersecurity:

> What are the responsibilities of a lawyer if they believe their client confidential information has been compromised by a cybersecurity intrusion?

The answer to that question can be found, in part, in **Rule 1.4**, which is the general rule on communicating with clients. It provides in relevant part:

> "RULE 1.4 - COMMUNICATION
>
> (a) A lawyer shall:
>
> …
>
> (3) keep the client reasonably informed about the status of the matter;
>
> …
>
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

In 2010, the New York State Bar Association expressed the view, in Opinion 842, that lawyers had a duty to advise clients of a breach of a third-party data storage systems (i.e., the "cloud"):

> "If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, *or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.* See Rule 1.4 (mandating communication with clients); see also N.Y. State 820 (2008) (addressing Web-based email services)." (Emphasis added)

In 2018, based in part on its version of Model Rule 1.4, the American Bar Association in Formal Opinion 483 discussed the issue of the duty to advise a client of a data breach.

> "When a data breach occurs involving, or having a *substantial likelihood of involving, material client information*, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules." (Emphasis added.)

And for a general discussion of the issue of securing client-protected information, see ABA Formal Opinion 477R, "Securing Communication of Protected Client Information." That Opinion discussed in very simple terms various cybersecurity issues, including the duties to supervise lawyer and non-lawyer staff under Rules 5.1 and 5.3. The duties to supervise include the duties to educate staff on conduct that could compromise client confidential information.

Working Remotely

a) In its Formal Ethics Opinion 2020-300 (2020), the Committee on Legal Ethics and Professional Responsibility of the Pennsylvania Bar Association discussed some of the ethical issues that arise for lawyers and their staff when working remotely and recommended best practices. The Opinion focused on the duty to provide competent representation and protect client confidentiality, and reminded lawyers that, when working remotely, they were under the same obligations to maintain client confidentiality as when working within a traditional physical office.

b) The Opinion noted that lawyers have an obligation, as part of their duty to provide competent representation, to understand the risks and benefits of technology and to use appropriate technology to protect the confidentiality of communications in both physical and electronic form. According to the Opinion, a lawyer's "duty to understand the risks and benefits of technology includes the obligation to safeguard client information (1) against unauthorized access by third parties[; and] (2) against inadvertent or unauthorized disclosure by the lawyer or other persons subject to the lawyer's supervision."

c) With regard to electronic communications such as email, the Opinion expressed the view that lawyers "may need to take additional measures to prevent information from being accessed by unauthorized persons."

d) With regard to physical work material such as paper files and other client-related documents, the Opinion stated that lawyers "should make reasonable efforts to ensure that household residents or visitors who are not associated with the attorney's law practice do not have access to these items."

e) The Opinion stressed the importance of shielding confidential telephone conversations from smart devices such as Amazon's Alexa and Google's voice assistants:

> "[S]mart devices such as Amazon's Alexa and Google's voice assistants may listen to conversations and record them.

> Companies such as Google and Amazon maintain those recordings on servers and hire people to review the recordings. Although the identity of the speakers is not disclosed to these reviewers, they might hear sufficient details to be able to connect a voice to a specific person."

f) The Opinion recommended the following best practices for remote work by lawyers and law firm staff:

- "Specifying how and where data created remotely will be stored and, if remotely, how the data will be backed up";
- "Requiring the encryption or use of other security to assure that information sent by electronic mail [is] protected from unauthorized disclosure";
- "Using firewalls, anti-virus and anti-malware software, and other similar products to prevent the loss or corruption of data";
- "Limiting the information that may be handled remotely, as well as specifying which persons may use the information";
- "Verifying the identity of individuals who access a firm's data from remote locations";
- "Implementing a written work-from-home protocol to specify how to safeguard confidential business and personal information";
- "Requiring the use of a Virtual Private Network or similar connection to access a Firm's data";
- "Requiring the use of two-factor authentication or similar safeguards";
- "Supplying or requiring employees to use secure and encrypted laptops";
- "Saving data permanently only on the office network, not personal devices, and if saved on personal devices, taking reasonable precautions to protect such information";

- “Obtaining a written agreement from every employee that they will comply with the firm’s data privacy, security, and confidentiality policies”;

- “Encrypting electronic records containing confidential data, including backups”;

- Avoiding the use of unsecured public internet/free Wi-Fi, which are vulnerable to hackers, for activities that involve accessing or transmitting confidential or sensitive data;

- Using strong, i.e., complex, passwords to protect data and devices;

- Not using USBs, flash drives or other external devices unless owned by the lawyer or provided by a trusted source; and

- Only accessing websites that use enhanced security protocols, i.e., “https://” addresses.

g) The Opinion also recommended that lawyers ensure that their video conferences were secure, and noted that the FBI issued a warning about teleconference hijacking during the COVID-19 pandemic and had recommended that users take the following steps “to mitigate teleconference hijacking threats”:

“• Do not make meetings public;

- Require a meeting password or use other features that control the admittance of guests;

- Do not share a link to a teleconference on an unrestricted publicly available social media post;

- Provide the meeting link directly to specific people;

- Manage screensharing options. For example, many of these services allow the host to change screensharing to ‘Host Only;’

- Ensure users are using the updated version of remote access/meeting applications.”

A *VERY BASIC* PRIMER ON CYBERSECURITY CONCEPTS

2023 was the worst year on record for cyberattacks on law firms, and a recent study revealed that there were 1.6 million records affected and an average ransomware demand of $2.47 million in 2023. Law360, London (August 1, 2024) "2023 Worst Year Yet For Cyberattacks On Law Firms: Study."

The Basics of Understanding How to Secure an IT Network

- What is an office network?
- What is an antivirus product and what are its limitations?
- What is a firewall?
- What are the points of intrusion where a lawyer's confidential information can be compromised?
- Do telephones and cell phones pose a cybersecurity threat?
- What are the remote access options? E.g., Citrix, GoToMyPC and AnyDesk.

The "Cloud"

- In simple terms, what is the "cloud"?
- Are there "hardware" or monthly upkeep financial benefits to the cloud?
  - Rental costs; hardware costs?
  - Avoiding back-up costs?
- How do "cost" issues impact the small firm versus the big firm?
- What is the concept of the "virtual workstation"?
- *What is the cybersecurity risk profile of these various alternatives?*

Cybersecurity Education Made "Somewhat Simple"

- Social engineering attacks: educating staff to not be "lured" into a hack.

- Carefully examining a client's email address that may be "spoofed."

- Inconsistencies in a familiar name which does not match a domain name.

- The new threat of the "DropBox" hack.

Critical Action Items for Law Firms

- Keep software up to date.

- Patch any vulnerabilities as soon as you become aware of them.

- Make backups of the backups.

- Give all employees regular cybersecurity training.

- Have a clear plan of action in case the worst happens.

- ***If anyone in the law firm is using a mobile app, make sure that the app accesses only non-confidential information on the device.***

- Consider issuing firm-owned devices that are capable of remote locking or clean-swiping. Make it clear in the firm's Employee Handbook that all data on such devices belongs to the firm.

- Implement strict control of administrator rights which control access to the firm's/clients' confidential information and make sure that all passwords and PINS for the firm and it staff are stored in secure applications such as 1Password.

- Regularly run up-to-date anti-malware programs on individual computers and servers on the firm's network.

- Check expert websites (such as www.us.cert.gov) and your firm's software vendors' websites regularly for alerts about new vulnerabilities and have policies for installing vendor-approved patches to correct problems.

- Restrict employees' ability to download unauthorized software. Software downloaded to devices which connect to a firm's network (computers, smartphones and tablets) could be used to distribute malware.

- Scan computers on your firm's network to identify and profile the operating system and open network services. If you find services that you do not need, disable them to prevent hacks or other security problems. For example, if email service or internet service or an internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to machines.

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords – such as common dictionary words – can be guessed easily, insist that employees choose passwords with a mix of letters, numbers and characters. Require that an employee's username and password be different, and require password changes when appropriate (e.g., following a breach).

- Explain to employees why it is against firm policy for employees to share their passwords or post them near their workstations.

- Use password-activated screen savers to lock employee computers after a period of inactivity.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.

- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

- Use a firewall to protect your computer from hacker attacks while it is connected to a network, especially the internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.

- Determine whether you should install a "border" firewall where your network connects to the internet. A border firewall separates your network from the internet and may prevent a hacker from gaining access to a computer on the network where you store sensitive information. Set "access controls" – i.e., settings that determine which devices and traffic get through the firewall – to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review these controls periodically.

- Determine if you use wireless devices such as smartphones, tablets or cell phones to connect to your computer network or to transmit sensitive information. If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.

- Encrypt the information you send over your wireless network, so that nearby attackers cannot "eavesdrop" on these communications. Look for a wireless router that has Wi-Fi Protected Access 2 (WPA2) capability and devices that support WPA2.

- Use encryption if you allow remote access to your computer network by employees or by service providers. Consider implementing multi-factor authentication for access to your network.

- Have a procedure in place for making sure that workers who leave your firm no longer have access to sensitive information. Terminate their passwords and collect keys and identification cards as part of the check-out routine.

- Teach employees about the dangers of spear phishing – i.e., emails containing information that makes the emails appear legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information. When verifying, do not reply to the email and do not use links, phone numbers or websites contained in the email.[1]

- If a law firm is involved in transferring more information than can be accommodated in simple email transfers, the firm will likely have to use secure file transfers or share data via links to a common cloud depository. Using multi-factor authentication is important because it limits the risks of exposure by requiring a secondary category of credentialing in the event that the primary credentials are compromised. Multi-factor authentication can consist of something the user has (such as a smart card) or something the user knows, in addition to a password. Daniel B. Garrie, Michael Mann and Leo M. Gordon, "Cybersecurity In Multidistrict Litigation," New York Law Journal, June 18, 2024.

[1] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

- When disposing of old computers and portable storage devices, use software for securely erasing data. These software programs, which are usually called wipe utility programs, are inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually is not sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.

MORE FROM FORBES

May 05, 2025, 10:03am EDT
Google Issues New Windows Captcha Security Alert — Don't Be Fooled

May 05, 2025, 09:00am EDT
Apple Passwords Attack Warning — Do Not Install This Update

May 05, 2025, 06:32am EDT
Government Security Warning Issued As Pas 2FA Hackers Strike

→

INNOVATION > CYBERSECURITY

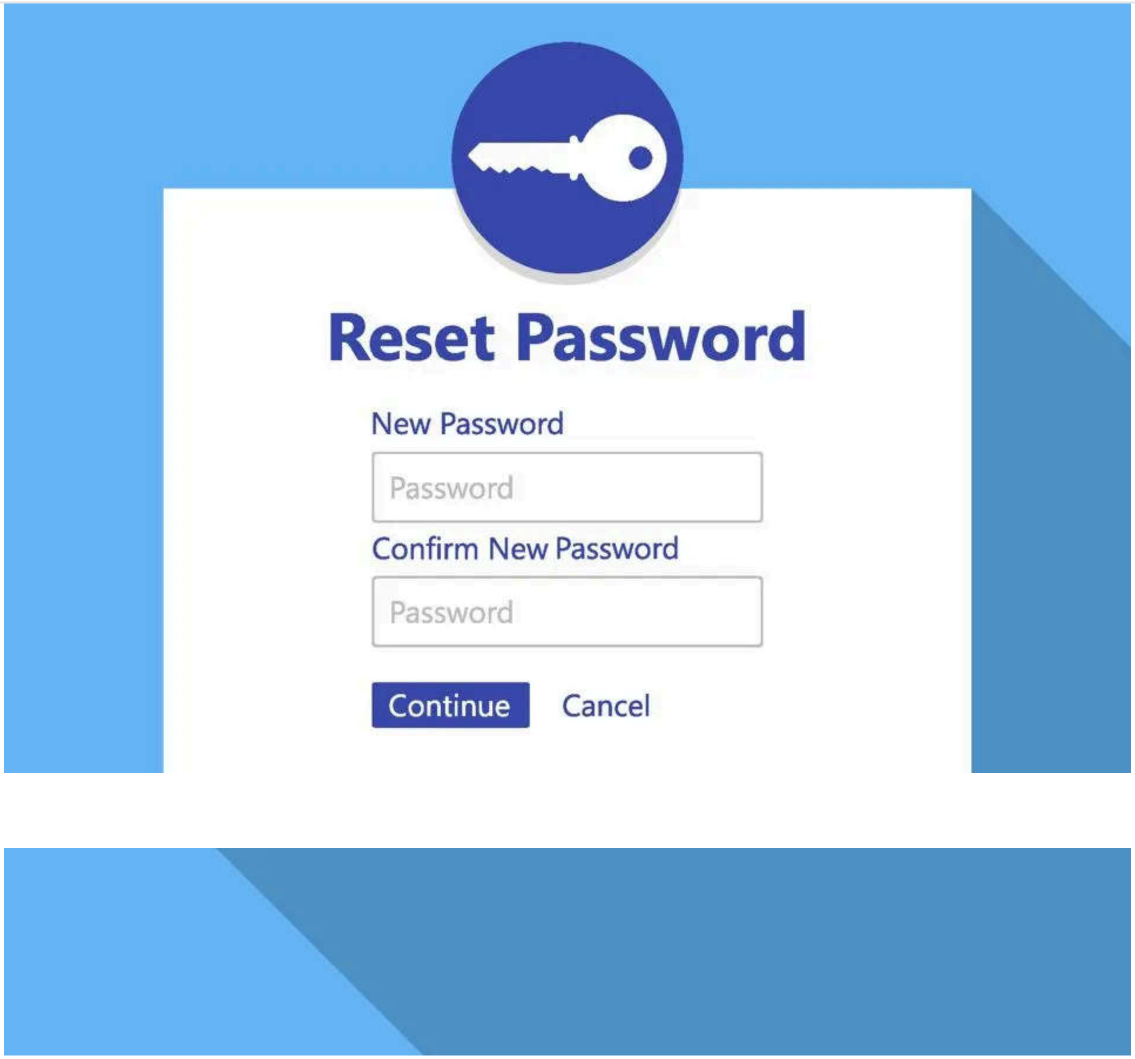
Confirmed — 19 Billion Compromised Passwords Published Online

By Davey Winder, Senior Contributor. ⓘ Davey Winder is a veteran...

Follow Author

May 05, 2025, 10:35am EDT

Share Save Comment 1



19 billion exposed passwords analyzed and it's not good news.
GETTY

Update, May 5, 2025: This story, originally published May 3, has been updated with details of an open letter to the cybersecurity industry asking why the phishing threat behind the stolen passwords epidemic has yet to be fixed.

In just the last few months, I have reported on confirmed lists of stolen passwords being made available on the dark web and in criminal forums that have risen from 800 million to 1.7 billion and even as high as 2.1 billion, mainly thanks to the rise and rise of infostealer malware attacks. But a new report has just blown even those shockingly large statistics out of the water with an analysis of 19 billion such passwords that are available online

FORBES

Apple Passwords Attack Warning — Do Not Install This Update

By **Davey Winder**

The 19 Billion Exposed Passwords Hacking Problem

Imagine having access to 19,030,305,929 passwords that were compromised by leaks and breaches over the course of 12 months from April 2024 and involving 200 security incidents. Imagine that only sources where email addresses were available for consumption alongside the stolen password were included in this massive database. Oh, and forget about including any of those word-list compilations, such as RockYou, that regularly do the rounds but are about as useful to a criminal hacker as a chocolate router. Finally, get to grips with the fact that this dataset only includes passwords that have become publicly available in criminal forums online. Once you digest all of this, you can appreciate how huge, in all senses of the word, this really is, especially to any hacker with criminal intent.

The analysis, published May 2 by the Cybernews research team, makes for truly eye-opening reading. It's so wide-ranging and security-scary in equal measure that it's hard to know where to start, so the beginning seems as good a place as any: password laziness and reuse. Of the 19,030,305,929 passwords that ended up exposed online, only 6% of them, or 1,143,815,266 if you like to be precise, were unique. Switch that around to 94% of them being reused across accounts and services, whether by the same or different people is moot, and you can see why the average cybercriminal gets very excited about the hacking potential such lists provide.

Now throw in that 42% of the passwords were short, way too short, being only 8-10 characters in length. That now opens up the hacking potential to brute force attacks as well as credential stuffing. Ah, yes, and it just keeps getting worse; 27% consisted of only lowercase letters and digits, no special characters or mixed case. Sigh.

FORBES

Government Security Warning Issued As Password And 2FA Hackers Strike

By **Davey Winder**

MORE FOR YOU

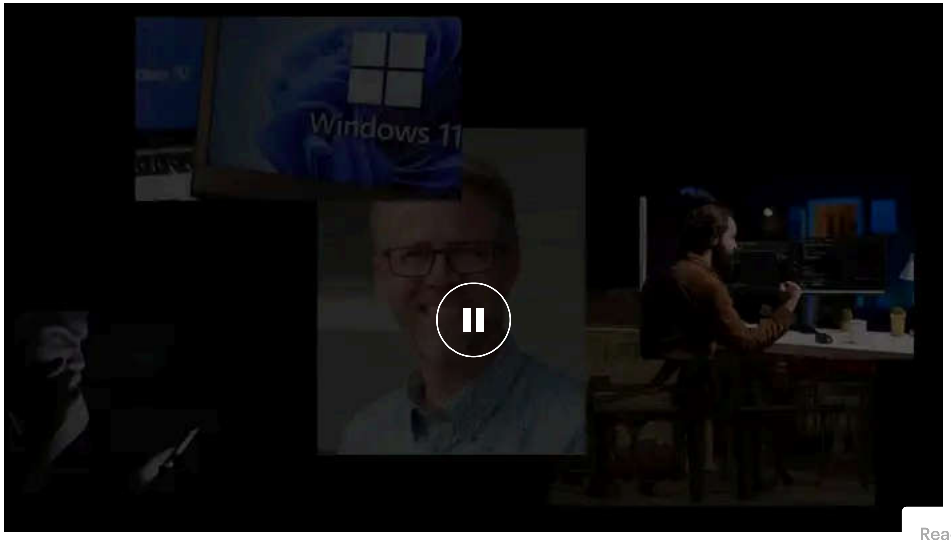
Today's NYT Mini Crossword Clues And Answers For Monday, May 5th

Delete Any Texts On Your Phone That Include These Messages

Microsoft Confirms You Cannot Cancel New Windows PC Update

Act Now To Mitigate The Stolen Passwords Threat

According to Neringa Macijauskaitė, an information security researcher at Cybernews, "the default password problem remains one of the most persistent and dangerous patterns in leaked credential datasets." The analysis revealed that there were 53 million uses of admin and 56 million of password, for example. Changing these is one quick way to help mitigate against hackers, as Macijauskaitė said, "attackers, too, prioritize them, making these passwords among the least secure."



Not reusing your passwords, ever, not at all, is another prime mitigation recommendation. "If you reuse passwords across multiple platforms, a breach in one system can compromise the security of other accounts, creating a domino effect," Macijauskaitė warned. Meaning that even without any existing system compromise, Macijauskaitė concluded. “These fresh datasets enable waves of highly effective credential-stuffing attacks, often bypassing traditional security defenses.”

FORBES

Apple Passwords Attack Warning — Do Not Install This Update

By **Davey Winder**

An Open Letter To The Cybersecurity industry — Stopping The Stolen Passwords Problem

Paul Walsh, CEO of MetaCert and co-founder of the W3C Mobile Web Initiative in 2004, knows a thing or two about the problem of malicious messaging and has been involved in the creation of internet standards to protect against it. In conversation, Walsh told me that the latest national SMS phishing test carried out in March by MetaCert and including carriers such as AT&T, Verizon, T-Mobile and Boost Mobile, was as disappointing as it was expected. “Every phishing message was still delivered,” Walsh told me, “none were blocked, flagged, or rewritten.” This is, to say the least, given that the vast majority of phishing platforms are now developed to target mobile devices, overtaking email in this regard in 2024 according to ProofPoint. When you consider that phishing attacks, on whatever platform, are the starting point for most cyber attacks, it’s no great leap to realize that the compromised passwords problem could be drastically reduced, if not stopped dead, by addressing the social engineering issue. Walsh has now written an open letter to the cybersecurity industry asking why the SMS phishing problem hasn’t been solved ages ago?

“The cybersecurity industry has no shortage of experts in email security, endpoint protection, or network defense,” Walsh said, “but when it comes to SMS infrastructure and security, there is a distinct lack of deep expertise.” His letter, therefore, is a call to action by security vendors who have “built multi-billion-dollar businesses on stopping phishing in email and corporate networks,” Walsh said, “yet the most trusted communication channel on the planet — SMS — remains an open, unprotected target.” Walsh demands that the same effort that has been made to address email security must now be made for the SMS vector because, he concluded, “criminals have already moved in full force, and the industry is failing to respond.” Unless this happens, and happens with the full might of the cybersecurity industry behind it, I fear that I will be reporting about the compromise of user passwords for some time to come yet.