Staying the Course During the COVID-19 Pandemic

March 20, 2020
by Sheila Blackford

Most law offices are operating with a skeleton crew onsite to receive, sort, scan, and deliver mail that is important for lawyers to continue practicing law by working from home. Other lawyers who are solos without support staff are working from home and visiting their law office to retrieve mail in the night or very early morning, daily or semi-weekly.

As of now, all deadlines and statutes of limitation currently remain in place. Until the State Judicial Department issues any changed rulings, adhere to the deadlines and SOLs affecting your personal cases.

During this time period of uncertainty, practice the precautions of social distancing to decrease the spread of COVID-19 while continuing to practice law.

Here are some steps you can do for as long as feasible:

1. Designate one person to go to the office when no one is present to open, sort, scan, and distribute the mail.
2. The person designated to process incoming mail and deliveries should wear a mask and protective gloves while handling mail and packages.
3. Instruct this designated person to thoroughly wash their hands, before and after touching surfaces.
4. Consider that the safest time to enter the office when no one is present will likely be very early in the morning or late in the night, if common sense tells you are not imperiling your physical safety or that of anyone else's.
5. Bookmark the website for the Oregon Department of Justice for the latest information. Chief Justice Walters issued a press release March 13 providing court guidelines on how to respond to the COVID-19 pandemic which can be read here: https://www.courts.oregon.gov/news/Documents/Covid-19News_3_13_20.pdf

© 2021 Oregon State Bar Professional Liability Fund. All Rights Reserved.

RESOURCES FOR WORKING REMOTELY IN THE AGE OF COVID-19

1. **Get your work-at-home game plan together.** For many lawyers, it feels unsettling to change to an extended work-at-home status. If you remember your favorite time management and office organization tips, dust them off because they will help you to preserve your optimism and focus on helping your clients and yourself. This blog post provides some good ideas to reassure us that we can creatively translate our work function from the office to our new work-at-home process: "Planning for a Shift to Remote Work? Tips for Staying Productive When Working from Home," https://www.govloop.com/community/blog/planning-for-a-shift-to-remote-work-tips-for-staying-productive-while-working-from-home/.

2. **Expand your methods for communicating with clients.** Not being able to meet with your clients in person does not need to put up a barrier to maintaining your relationship and communicating effectively. Emails and phone calls are helpful, but the ability to see each other when you communicate is necessary in an ongoing attorney/client relationship. Certainly the opportunity to chat via Facetime on your Apple devices is very easy. This blog post has excellent tips for carrying on your meeting via video conferencing: "Working and Meeting in the Age of Social Distancing," https://osbplf.org/inpractice/working-and-meeting-in-the-age-of-social-distancing-/.

3. **Remote access.** Having access to client files and programs on your work computer while working from home is an important part of setting up. This type of remote access requires particular technology such as remote desktop and a virtual private network (VPN). This blog has more information on remote access: https://www.osbplf.org/inpractice/remote-access-for-lawyers--remote-desktop-protocol-rdp-and-virtual-private-network-vpn/.

4. **Tune in to the best news channels.** Gather your sources for reliable news about COVID-19. Although it is tempting to throw "COVID-19" into Google's search box, what comes up may bury you and send you into an extended derailment reading news about the virus. Two essential reliable sources of information include the World Health Organization (www.who.int) and the Centers for Disease Control and Prevention (www.cdc.gov), which can give you tools for keeping you and your family healthy. The World Health Organization has also launched "Health Alert" to bring COVID-19 facts via the WhatsApp. Send 'hi' on WhatsApp to +41 79 893 18 92 to start the conversation.

5. **Disarm the myths about the coronavirus**. The longer we try to make sense of the COVID-19 pandemic, the more we find ourselves being updated by well-meaning but misinformed individuals. When it comes to the coronavirus, rumors become myths and the World Health Organization is there to stop the "fake news" spreading as fast if not faster than the virus itself. A favorite resource to bookmark is the WHO Mythbusters (https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters).

6. **Learn how to identify the symptoms to be concerned about**. You sneeze, you cough, you Google "Coronavirus symptoms" so you will know when it is time to call the doctor. The Centers for Disease Control and Prevention has a helpful "Coronavirus Self-Checker" so that you can get informed about your symptoms and what to do if you have been exposed: https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/steps-when-sick.html.

7. **Get a plan for picking up mail so you don't miss a deadline**. "You've got mail" was a welcome announcement in the early days of email on AOL. You may have conquered your email inbox but are beginning to get seriously distressed at the thought of unopened mail piling up, including notices of deadlines. "Staying the Course During the Covid-19 Pandemic," has some ideas to help you: https://www.osbplf.org/inpractice/staying-the-course-during-the-covid-19-pandemic/.

8. **Set up a secure way to share documents with clients**. Sending documents back and forth with your client doesn't have to be done inefficiently or insecurely. A client portal may soon become your favorite way to share confidential documents with your clients. Here is a blog post to help you get started: "Client Portals: Take Control of Client Communication," https://www.osbplf.org/inpractice/client-portals--take-control-of-client-communication/.

9. **Make it easy to get paid**. If you are not already set up for sending secure invoices that can be paid with a click of a button or having a special website link in your client portal for credit card payments, now is a good time to get set up. Look at your case management program to determine how it can enable providing clients with accurate, timely billings and for streamlining being paid. If you find that the included bill paying feature doesn't meet you and your client's needs, consider standalone billing programs such as Bill4Time, Time59, and TimeSolv.

10. **Getting set for remote signing**. Make online signing available for clients to sign their fee agreement, engagement letter, other documents, and forms. Electronic signature services like DocuSign, signNow, and HelloSign let clients sign on their computer or mobile device without having to print, scan, and email or mail back to you.

11. **Offer online scheduling.** Eliminate calling or emailing back and forth to schedule appointments by using an online scheduling tool that allows new clients, existing clients, and others to make their own appointment with you based on your availability. Just provide a link to the online calendar or embed it right into your website. Common online scheduling tools include Calendly, Acuity Scheduling, and ScheduleOnce.

12. **Stay in touch with your team**. If you miss the weekly huddle with your practice team, you can still gather the groups. Two ideas: Slack can serve as a private posting platform that lets you set up channels— maybe a channel for one department or a channel for each client matter. You can even add in video meetings. Zoom is a video conferencing or webinar platform that can help you communicate with greater ease and speed.

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund, except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices. © 2020 OSB Professional Liability Fund.

CONFIDENTIALITY IN THE OFFICE

Oregon lawyers are bound by ethical rules which require them to preserve confidential client information. This is the cornerstone of the legal profession. If confidentiality is not observed, it not only results in injury to the client, but contributes to loss of trust and credibility in the legal profession.

Rule 5.3 of the Oregon Rules of Professional Conduct provides:

"With respect to a nonlawyer employed or retained, supervised or directed by a lawyer:

(a) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
(b) …a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer…"

Legal staff must understand that every piece of information about clients, whether written or unwritten, which comes to their attention in their job must be treated with utmost confidentiality. If this confidentiality is not observed strictly, the result will not only be injurious to the client, but it may also subject the lawyer to possible disciplinary action for breach of the Oregon Rules of Professional Conduct. A further consideration is that any leak of confidential information by legal staff regarding a client could lead to the destruction of a lawyer's reputation so that no client would utilize the lawyer's services. The lawyer could lose his or her livelihood.

Consider some circumstances in which legal staff could unconsciously or inadvertently violate this confidential attorney-client relationship:

1. Confidential client information could be disclosed to legal staff of Firm A by the legal staff of Firm B during lunch or some other social occasion. Firm A might represent a party adverse to the client of Firm B and the discussion may have revealed important information which could be harmful to the client of Firm B.

2. Carelessness in mailing, emailing, or faxing information of a confidential nature could inadvertently result in an important communication intended for a client being directed to an adverse party or to someone who could use this information against the client.

3. A poorly maintained desk and/or working area with open files and client documents on the desk, or confidential documents on the computer screen, could allow an unauthorized person to obtain confidential client information simply by sitting in the waiting room or going by the desk to pick up a magazine from a table.

4. Confidential client information can be released by answering telephone questions from a purported relative of a client, or responding to other official-sounding requests of a third party, without first consulting the lawyer.

5. Copies of client documents can be inadvertently released to third parties who walk in the office and request them without the lawyer's explicit instructions to do so.
6. Discussions with friends, relatives, or spouses about work situations or cases can release confidential client information which may unknowingly be transmitted to other parties.

CONFIDENTIALITY IN THE OFFICE

To emphasize the sensitive nature of working in a law office, legal staff should carefully read and sign this Confidentiality Pledge or Confidentiality Agreement acknowledging their understanding of the confidential nature of the legal profession.

Confidentiality Pledge

I, [*name*], having accepted the position of [*legal secretary, legal assistant, receptionist, bookkeeper, etc.*] in the law offices of [*name*], acknowledge that I fully know of the confidential nature of my position and of my obligation to the clients of this law firm and to the lawyers of this law firm to safeguard such information with which I am entrusted, and to release such information only on the authorization of the lawyer handling the client's case. I understand that any breach of confidential would constitute a failure to fulfill my employment obligations and could be harmful to clients of this firm.

I pledge that I will strictly maintain the confidentiality of all client information which comes to my attention, and that upon the expiration or termination of my employment with this law firm I will reveal none of such confidential information unless specifically authorized and directed to do so by the appropriate lawyer or lawyers of this law firm.

_____ _____

(Date) Employee's Signature

CONFIDENTIALITY IN THE OFFICE

Confidentiality Agreement

It is impossible to overstate the importance of the attorney-client privilege. So sacred is the relationship between lawyer and client that information given to the lawyer by the client is "privileged communication" -- the lawyer cannot be compelled to testify about it. This bedrock principle between attorney and client creates the trust and confidence required for proper representation. Our firm's clients are the most important people with whom we interact. Without them, the law practice cannot survive.

In your work with [*firm name*], you will undoubtedly have access to confidential client information. It is one of your most serious responsibilities you in no way reveal any such information and that you use it only in performing your duties. If you have doubts about what might be confidential information or violating trust, seek advice from the Managing Partner.

Optional Additions (use as applicable)

(a) Employees are responsible for the internal security and safekeeping of such information. You will read and follow the policies on protecting information.

(b) Employees are prohibited from engaging in securities transactions based on information not available to the general public and that, if known to outsiders, might affect their investment decisions. The dissemination of such information to others who might make use of that knowledge to trade in securities is also prohibited.

(c) Proprietary and confidential information can take many shapes, including, but not limited to the names of clients the firm represents or the fact of their visits to the office, documents, notes, overheard conversations, tapes, diskettes, personal observations, records, research, blueprints, financial statements, licensing agreements, trust funds, criminal records, strategic plans, product developments, emails, pending patents, research proposals, chemical or biologic formulae, or allegations made by others about our clients.

(d) Employees will have to sign a statement of confidentiality at the time of hire and annually throughout their term of employment to acknowledge their awareness of, and to reaffirm their commitment to, this policy.

(e) Employees are expected not to divulge, during their term of employment or after their employment is terminated, any information confidential or proprietary information acquired during their employment.

(f) Information regarding the operations, activities, and business affairs of the firm are also to be kept confidential and not discussed with outsiders.

(g) Employees found to violate the firm's confidentiality policies are subject to disciplinary action, including termination, and may also be subject to civil and/or criminal penalties for violations of applicable securities laws.

(h) In preserving the security of files and information, the following are to be observed:

1 Disclosing information -- Information in office files should never be disclosed, except upon express authorization of the lawyer handling the case. Sometimes, a written authorization from the client may be sufficient authority.

CONFIDENTIALITY IN THE OFFICE

2 Delivery of documents -- Documents or files are to be turned over only to persons properly identified or vouched for and then only in return for a signed receipt and when authorized by the lawyer handling the matter.

3 Use of offices -- In a lawyer's absence, no client, visiting attorney or stranger may use a lawyer's office for any purpose unless a member of the office staff is present the entire time. Even if monitored, the desk should be kept so that files, papers, and correspondence are not exposed. Under no circumstances should a client, visiting attorney, or stranger place a telephone call from a lawyer's office, unless that lawyer gives permission.

4 Disposal of confidential papers -- All confidential papers should be destroyed when no longer needed. This includes rough drafts or interim copies. Paper shredders are available throughout the office for that purpose.

5 Revealing client's business -- One client's business is never to be discussed with another client. As a general policy, it is best not to mention one client's name to another. The temptation to brag about our important clients should be resisted.

6 Discussing firm matters -- Do not discuss client matters when clients or visitors are present, particularly in the reception or kitchen areas. A visitor or client who overhears information about another of our clients will feel that his or her personal affairs will receive the same lax treatment.

7 Exposure of documents -- Copies of correspondence, pleadings, interoffice memoranda, or any other documents should be placed either on a designated tray on the secretary's desk or on the lawyer's desk. Tray covers are provided by the firm.

I have read, understand, and agree to the provisions herein.

_____ _____

(Date) Employee's Signature

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund except that permission is granted for Oregon lawyers to use and modify these materials for their own practices. © 2019 OSB Professional Liability Fund

inPractice
Practical Advice for Oregon Lawyers

Remote Access for Lawyers: Remote Desktop Protocol (RDP) and Virtual Private Network (VPN)

May 31, 2019
by Hong Dao

As lawyers embrace the trend to work offsite, remote access becomes an important tool. Remote access refers to the ability of one computer to remotely access information on another computer or network. This functionality lets lawyers access their applications, folders, and files on their work computer while working from home or somewhere offsite. Bigger law firms usually have their IT department set up remote access for their employees. Small firms and solo attorneys are typically on their own when it comes to remote access.

There are different ways to set up remote access, and this blog post will cover two main options: (1) Remote Desktop Protocol (RDP) and (2) Virtual Private Network (VPN). Explore both options and choose one that offers the maximum security to protect client or other kinds of information.

Remote Desktop Protocol

Remote Desktop Protocol, also referred to as screen sharing, is a method that allows users to connect to another computer and use it as if they were sitting in front of that computer. This can be implemented using the native application in most computers' operating systems or using third-party remote desktop software applications.

Windows Remote Desktop

Microsoft originally developed Remote Desktop Protocol (RDP) to maintain and troubleshoot their servers. RDP has since been made available on all Windows computers to allow users remote access to another computer on your local network or over the Internet. But only computers running on the Professional, Enterprise, or Ultimate editions of Windows have what is called an RDP server that allows any computer to connect to that computer. Computers with the Home edition of Windows do not have an RDP server. This means that other computers cannot connect to it, but it can connect to a Pro (and above) edition.

Instructions for setting up remote desktop for computers in your local network can be found at the Microsoft website here for Windows 7 (which Microsoft will no longer support in January 14, 2020) and here for Windows 10.

Setting up remote desktop to a computer outside your network can be complicated. You will need technical assistance with setting up, configuring, possibly installing parts, and performing other steps if you are not tech-savvy. Have an IT person help you if this is what you want to do.

Mac Screen Sharing

Mac computers also have built-in remote desktop capability. Instructions to set up screen sharing are available at the Apple website here. Apple also has an advanced remote desktop solution suitable for institutional use for $79.99 called Apple Remote Desktop.

Chrome Remote Desktop

Chrome users can install the Chrome Remote Desktop extension on their PC or Mac computer for remote desktop. Instructions on how to do this are available here.

Security Concern

When remote desktop connection is made over the public Internet, it exposes your data to potential attacks because the transfer of data between the remote computer and your home computer is not secure. Lawyers should use VPN (discussed below) to secure your connection and Internet traffic, or you may consider using bundled third-party RDP software.

Third-Party RDP Software

Third-party remote desktop software applications let you connect with another computer with the added benefit of security and encryption. All remote connections and data transferred during the session are encrypted using industry standard encryption. This is important for lawyers working on client files from afar and needing to maintain the confidentially of their client data. Some popular programs include LogMeIn, GoToMyPC, and RemotePC.

All these programs have easy installation, mobile access, and many useful features not offered by the native programs. Some of the programs offer basic free plans. Lawyers should consider upgrading to the paid versions.

Virtual Private Network

You can also establish remote desktop using a VPN or Virtual Private Network. A VPN creates a virtual secure tunnel between your computer and a remote network via a VPN server. This server connects users to the Internet and imposes various security protocols. Your Internet traffic is then routed through that encrypted tunnel, and nobody can see through the tunnel to view or steal your data. It also provides anonymity and privacy. A VPN allows you to be anonymous while using the Internet because it hides your IP address (which identifies you and your location), so your data can't be traced back to you. It is used to thwart Internet surveillance and online tracking by your browser, your Internet service provider (ISP), or others.

Let's demonstrate the value of a VPN in the context of public Wi-Fi. Places like coffee shops, restaurants, hotels, and airports offer free public Wi-Fi. The open nature of a public Wi-Fi network allows other people on that network to see what you're doing online and capture your passwords, banking information, credit card number, and other information about you or your clients. A VPN encrypts your data transferred over that unsecured network to ensure no one can intercept it.

Due to the security and privacy offered by a VPN, it's a good idea to use the secure tunnel to access remote desktop. Popular VPN providers include NordVPN, Tunnel Bear, OpenVPN, and ExpressVPN. After registering and paying for service, users download and install the program to their computer. Then users launch the VPN application and access their remote desktop via the native RDP applications discussed above.

Whatever program you use, keep in mind one important difference between RDP and VPN. RPD allows access and control to a specific remote *computer* and all the resources on that computer. A VPN, on the other hand, allows access to a remote *network* and the resources shared on that network, and it provides anonymity and privacy, which RDP does not. RDP has security risks that can be reduced by using a third-party RDP software application or a VPN to encrypt data.

If all this information sounds too technical, you're better off hiring an IT person to help you set up remote desktop or determine which remote access options will work for you.

© 2021 Oregon State Bar Professional Liability Fund. All Rights Reserved.

inPractice
Practical Advice for Oregon Lawyers

Working and Meeting in the Age of Social Distancing

March 16, 2020
by Hong Dao

In light of the spread of COVID-19, many lawyers are looking for ways to continue meeting with their clients and other parties while keeping some distance from them. Fortunately, we are in an age where technology makes it easy to implement social distancing efforts that many individuals and businesses are now undertaking. This blog post will cover two tools that will allow lawyers to work and maintain social distance: (1) video conferencing and (2) remote access.

Video Conferencing

Video conferencing is a great alternative to in-person meetings that saves on travel expenses and is fairly easy to use. It allows participants to hold online face-to-face video meetings using their computer or mobile device with built-in cameras, speakers, and microphones. It includes the ability to share screens and set up virtual conference rooms for attendees to click, join, and collaborate.

While there are many options for video conferencing services, this blog post will cover only a few services that offer a free plan in addition to their paid ones. Many video conferencing services share the same basic features, including:

- Conference call – offers audio-only meetings.
- Screen-sharing – allows other participants to view files even if they don't have the software needed to open the files on their computer. It helps boost collaboration when all participants are able to access and see the same information during the meeting.
- Recording - allows audio or video recording of meetings saved either to your computer or the cloud (in your account).
- Meeting duration – limits the duration of each meeting.
- Desktop & mobile access – allows participants to join the conference on their desktop computer or mobile device.
- Participant capacity – limits the maximum number of participants in each meeting.
- Online whiteboard – allows users to draw, write, and take notes for everyone to see.

Here is a comparison chart of some conferencing services. The chart includes features from their free plan as well as features from their paid service starting with the most affordable plan. Due to limited space, the chart does not include every feature. This chart also has links to the companies' security and privacy policies. A few services offer end-to-end encryption on their video calls (e.g., Cisco Webex and LifeSize) while others do not explicity state this on their website. Please do your own review of their security information and privacy policies.

Remote Access

Law firms that are asking their lawyers to work from home should provide some options for lawyers to access their files and other information on their work computer. This is probably not a problem for lawyers who save all of their client files in the cloud. Even if that is the case, there may still be desktop programs and applications on a lawyer's work computer that he or she needs to effectively work from home. This type of access typically requires the use of remote desktop technology. I've written a blog on different options for remote access available here.

New Possibilities

COVID-19 presents many challenges to lawyers as they may see their business dwindling. But this challenging time may provide an opportunity for lawyers to try something new—a different way to deliver legal services. Consider adopting some features of a virtual law firm to help you move your legal services online. For more information on what a virtual law firm is, please read my article titled *Beyond Brick and Mortar: Virtual Law Firms Shift*

Delivery of Legal Services Online published in the Bar Bulletin, January 2020.

I also recently presented a CLE on automating the client intake process that allows lawyers to do many tasks online, such as scheduling, payment, and signing. That CLE that is now available for free on the PLF's website. To order this CLE, click here or go to www.osbplf.org > CLE > Past > "More Than Just a Click: Automating the Client Intake Process."

-- Updated 4/2/20

© 2021 Oregon State Bar Professional Liability Fund. All Rights Reserved.

Video Conference Services Comparison Chart

Name	*Pricing*	Conference call	Video conferencing	Screen sharing	Recording	Meeting duration	Desktop & mobile access	Participant capacity	Online whiteboard	Security/privacy policy
Cisco Webex Meetings https://www.webex.com	Free plan	✓*	✓	✓*	X	No limit*	✓	Up to 100*	✓*	Security info here; Privacy info here.
	Paid plan $13.50/mo	✓	✓	✓	✓	No limit	✓	Up to 50	✓	
ezTalks https://www.eztalks.com	Free plan		✓	✓	✓	40 min for group		Up to 100	✓	Security info here; Privacy info here.
	Paid plan $10/mo		✓	✓	✓	Unlimited		Up to 100	✓	
Lifesize https://www.lifesize.com	Free plan (6 months)		✓	✓	X	No limit	✓	Up to 25	X	Security info here; Privacy info here.
	Paid plan $16.95/mo		✓	✓	Not at this plan	No limit	✓	Up to 100	At extra charge	
UberConference https://www.uberconference.com	Free plan	✓	✓	✓	✓	45 min	✓	Up to 10	X	Security info here; Privacy info here.
	Paid plan $15/mo	✓	✓	✓	✓	5 hr	✓	Up to 100	X	
FreeConference.com https://www.freeconference.com	Free plan	✓	✓	✓	X	No limit	✓	Up to 1000 for calls; up to 5 for web	✓	Security info here; Privacy info here.
	Paid plan $9.99/mo	✓	✓	✓	✓	No limit	✓	Up to 1000 for calls; up to 15 for web	✓	
Zoom https://zoom.us	Free plan	✓	✓	✓	X	No limit for 1:1; 40-min limit for group	✓	Up to 100	✓	Security issues recently in the news. Security info here; Privacy info here.
	Paid plan $14.99/mo	✓	✓	✓	✓	24 hr	✓	Up to 100	✓	

* = Free one month with these upgraded features when you sign up for a paid monthly or yearly plan. Original free plan does not require paid commitment but limits meetings to 40 min up to 50 people with no screen sharing, whiteboard and audio-call in.

inPractice
Practical Advice for Oregon Lawyers

Client Portals: Take Control of Client Communication

March 6, 2020
by Rachel Edwards

Client portals allow lawyers to interact with clients in a secure environment to accomplish tasks such as gathering information, sharing documents, and making payments for services. The word "portal" comes from the Latin term for a gate, meaning it maintains two functions. It opens to allow access but also closes to ensure security. Portals are designed to facilitate communication between attorneys and clients. Email is generally not a secure method of communication, and it can be challenging to sort through the vast number of emails we receive every day. Client portals add a layer of security and free up your inbox. These services are widely available in other professions, such as for doctors and accountants. They can be a valuable tool for lawyers, so consider implementing them into your practice if you haven't already.

Depending on the program, client portals contain various capabilities, including the following:

- Gathering information from clients
- Messaging with clients
- Sharing documents
- Setting appointments
- Making payments for services
- Sharing client-specific calendars
- Assigning tasks to clients
- Sending reminders to clients
- Tracking attorney time
- Document automation

Before choosing any particular program, consider the following factors:

1. **Whether you have or are considering practice management software.** If you already use a practice management program, look to see if it has a client portal. If you're considering using a practice management program, see if it has a client portal. Practice management portals allow for feeding of information into a client matter so all information is kept in one location.
2. **Know your goals.** Are you trying to facilitate communication with clients? Then find a portal that allows them to send messages so they aren't tempted to send an email or make a phone call. Are you seeking a way to simply exchange documents with clients? Then a standalone document exchange portal may suffice. Are you trying to increase fee collection? Then consider a portal that allows for electronic payment.
3. **Increase client accountability.** If you struggle with clients not completing requested tasks, such as providing discovery, find a portal that has an "audit" trail to track when clients viewed documents or took action.
4. **Always vet the vendor.** Client portals store information in the cloud, so be sure to vet the vendor in accordance with OSB Formal Ethics Opinion 2011-188. This becomes especially important if the program isn't designed for a law firm, because it may not provide the level of security you require. A secure portal assures that data is encrypted while transmitted.
5. **Be prepared to train clients or provide training materials.** Make sure you are familiar with the portal in case you need to explain it to the client. Or find out whether the program has training materials that can be given to the client rather than spending your time training them. And clients should be instructed to contact the portal company first if they're having trouble with it, and only contact the attorney if the issue is time-sensitive.

Below is a list of client portal providers you may consider:

1. Practice management software. The following practice management programs contain client portals and offer discounts to PLF members: Clio, CosmoLex, MyCase, PracticePanther, and Rocket Matter. Others include Filevine, Zola Suite, Smokeball, LEAP, and Actionstep.

2. Standalone client portals. If not using practice management software, there are standalone programs that contain certain portal capabilities:
    a. File-sharing: Citrix Sharefile, Microsoft Sharepoint, NetDocuments, Google Drive, Dropbox, Box, and iManage.
    b. Various capabilities: DirectLaw is a cloud platform that allows clients to accomplish tasks such as fill out documents, sign contracts, send messages to their attorney, pay bills, and access a customized calendar.

Client portals can reduce interruptions throughout the day by allowing clients to communicate via the portal rather than through phone calls or emails. It allows you to control how the client communicates with you, and to control how you manage your time. The key is to set expectations with your clients up front, letting them know that they need to use the client portal, and enforce that expectation if they try to use other methods of communication.

© 2021 Oregon State Bar Professional Liability Fund. All Rights Reserved.

inPractice
Practical Advice for Oregon Lawyers

Understanding Security When Using Cloud Storage

October 20, 2017
by Hong Dao

Lawyers increasingly rely on the cloud to store, share, and synchronize their client files. Many use Dropbox and Google Drive for this purpose. However, the use of these common cloud storage services presents some data security concerns. Issues of whether data is encrypted and who has access to the data make some lawyers understandably nervous about having a third party store their client information. The risk of malpractice exposure if client data is compromised or breached is something lawyers need to evaluate.

Before you choose to store your client data with an online third-party vendor, take some time to understand how that data is secured and protected. Encryption, which makes data unreadable, plays a big role in data protection. Data can be encrypted at several levels, but not all vendors encrypt data at every crucial level. A good cloud storage provider encrypts your data at three different stages to provide the most protection: (1) before it leaves your computer, (2) in transit to the provider's server, and (3) when it is stored on the provider's server.

My goal is to help you understand why encryption at each stage of data transfer is important. Then you can make an informed decision as to which provider to use. So let's look at the different stages in more detail without getting too technical.

First stage: Client-side encryption for data before transit

Before you transfer your data from your computer to the provider's server at their data center, you encrypt your data locally on your hard drive with a private encryption key using the provider's tool. You are the only one with the key. A copy is not shared with the provider, so it has "zero knowledge" of your key. Without knowledge of your key, the provider has no access to the data stored on its server. This is called client-side or zero-knowledge encryption. Encryption at this level is crucial because it makes all your files unreadable by everyone. Only you can decrypt the data using your key. The data is therefore protected against backdoor access and outside hackers because your key is not stored with the provider.

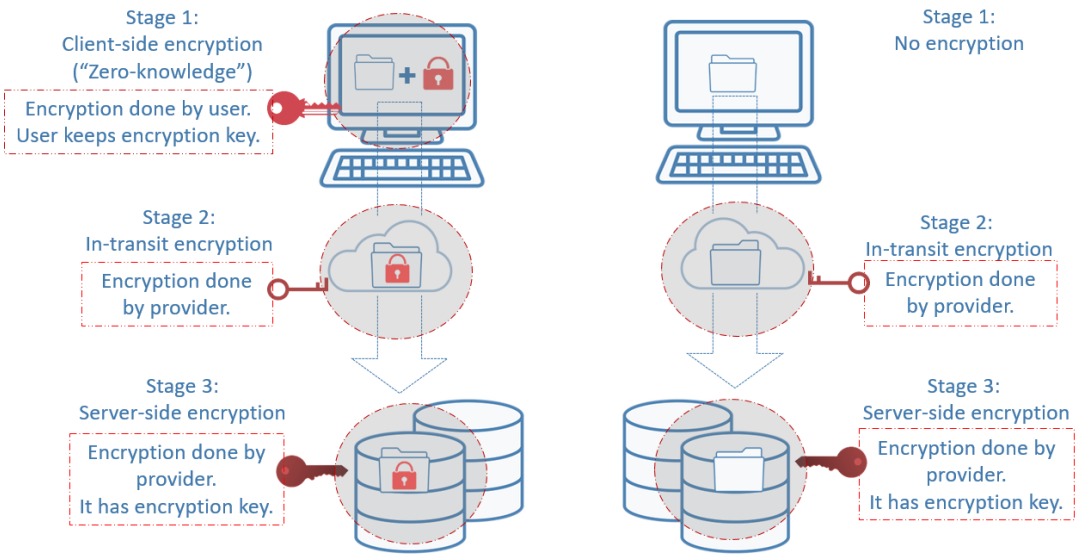
Second stage: Encryption for data in transit

Once your data is locally encrypted on your computer, it will be transferred to the provider's remote server. The transfer occurs over encrypted connections established by the provider. Encryption at this stage ensures your data is not vulnerable to interception while it's in motion. Client-side encryption doesn't prevent attackers from intercepting the transfer and seizing your encrypted data. Even though attackers may not be able to decrypt your data, they can still hold it hostage. In-transit encryption prevents this from happening and provides another layer of security for your data.

Third stage: Server-side encryption for data at rest

When your data reaches the provider's server where it will reside for an indeterminate period, it is secured with a third layer of encryption. Encryption at this stage is done by the provider. It stores and maintains the decryption key along with your data. This is called server-side encryption. Although the provider manages the decryption key at this stage, your data is still protected from provider access as long as you've used client-side encryption at the first stage.

Below is an illustration of what encryption looks like at the three stages and what it looks like when there is no client-side encryption at stage 1.



What does this mean for lawyers?

Almost all cloud storage providers offer encryption at the second and/or third stage. Only a handful offer encryption at all three stages.

This means that storage providers (e.g. Dropbox and Google Drive) who do not offer client-side encryption have the *ability* to access your data. This is something you want to seriously think about if you're storing sensitive or confidential client information on their servers.

What are your options?

You have many options to better protect your client data stored online. Below are a couple of practical options for lawyers.

Use zero-knowledge providers

Zero-knowledge cloud storage providers use encryption at all three crucial stages. Client- side encryption at the first stage lets you manage your own key. The upside of this is obvious: providers have no access to your data. The downside, however, is that if you lose or forget your key, your data is gone. You can't rely on the providers to reset the password for you or issue you a new password. They only have proof that you have your key, but they don't have the key itself. Other downsides include slow backup and recovery due to security measures in place.

If you want to use zero-knowledge storage providers, here are some you can look into: SpiderOak (U.S.), Terosit (Switzerland) Sync.com (Canada), pCloud (Switzerland), and MEGA (New Zealand).

Encrypt before you upload

If you choose to use Dropbox or a storage provider that doesn't offer client-side encryption, you should consider using third-party zero-knowledge software to locally encrypt the data yourself before you upload to the cloud. When you use the encryption software, only you, not the software provider, have the key to decrypt the files. Once the encrypted files are uploaded to the storage provider's server, there is no risk that it can access your data.

After downloading the software, you will set up your account and select Dropbox or whomever your cloud storage provider is. An encrypted drive connected to Dropbox will be created on your computer. When you transfer files to the encrypted computer drive, those files will be automatically encrypted and then uploaded to Dropbox through file synchronization. They will be stored there in their encrypted state. Beware that some user features such as file sharing may be limited when your data is encrypted.

Here are a few software programs that offer zero-knowledge encryption: Boxcryptor, ODrive, and Cryptomator Many other programs allow you to encrypt before uploading, but they are not zero-knowledge. They include NCrypted Cloud, Sookasa/Safemonk, and Safebox.

Always vet the vendors

Do your due diligence by vetting the providers. Research their reputation by reading online reviews and articles about them. See how long they have been in business and whether they serve lawyers. Review the terms of service and user agreement to ensure they comply with industry standards for preserving confidentiality and security of data. Use the resources below to help you do the vetting.

Resources:

- Online Data Storage Providers – PLF Practice Aid
- Encryption Made Easy: The Basics of Keeping Your Data Secure – OSB Bar Bulletin Article

© 2021 Oregon State Bar Professional Liability Fund. All Rights Reserved.

ONLINE DATA STORAGE PROVIDERS

ONLINE STORAGE GENERALLY

An online data storage provider is an Internet-based service that backs up your entire system automatically, and stores the data on the Internet in a secure form and location. You may see this process referred to as storing your data "in the cloud," Web-based data storage, or "software as a service" (SaaS).

Using Internet-based data storage for backup and recovery has generated significant discussion in legal circles. Before deciding to use a third party to store your electronic data, review the following:

- OSB Formal Opinion No. 2011-188,
- Safeguarding Client Information in a Digital World by Helen Hierschbiel, *Oregon State Bar Bulletin* (July 2010),
- The Ethics of Electronic Client Files: Floating in the Cloud by Amber Hollister, *Oregon State Bar Bulletin* (May 2017), and
- Understanding Security When Using Cloud Storage by Hong Dao, *InPractice* (October 20, 2017).

The data stored on your computer is the lifeline of your practice. Safeguarding that information is critical to your practice's survival, and to meeting your ethical obligations to your clients. Online data storage can provide access to, and protection of, your data that an offsite backup cannot. This is especially true if your offsite backup is stored in your same town or locale and a natural disaster strikes. A backup device at home or other local site would likely be inaccessible or damaged. In contrast, if you are displaced from your office by a localized disaster, Internet-based data storage allows you access to client documents and financial information as soon as you are able to access the Internet.

Despite potential advantages, many lawyers have reservations about using online data storage. Generally, security issues associated with storage are the main concern. Placing client information in the hands of third parties, the solvency of the provider, the security of the storage location, the method of storage, and the preservation of confidentiality are all reasonable concerns raised by lawyers. However, these concerns exist whether you store paper files in a storage facility or store electronic data with an online provider. With a paper storage facility, once you are confident the facility has no access to your stored documents or maintains your confidentiality and privacy, you turn over the boxes of client files for storage and periodic retrieval. Placing electronic client data in the hands of third parties who remotely upload it to their website is not any different. Proper security is crucial for each storage method. Unauthorized access can happen if a paper storage or an electronic storage site is not secure.

Similar to a physical storage center, an online storage center can provide the user with a special key to access electronically stored data. An online provider's security can be so restrictive that the user may be the only person who has the key. Storage this restrictive requires careful thought, planning, and safeguarding, as there is no access if the key is lost. Therefore, if you are the only key holder, store the key (usually a password) locally somewhere that is secure, such as a safe deposit box, as well as somewhere secure in another geographic area. Do not rely on your memory.

ONLINE DATA STORAGE PROVIDERS

Vet the Vendor

When choosing an online data provider for storage or backup, consider asking the vendor the following questions:

- Does the system offer the highest form of data encryption available in the United States: Advanced Encryption Standard (AES)?
- Does the system offer a private encryption key, held only by your office?
- Does the system encrypt all transmitted data at the source?
- Is data encrypted both at rest and in transit?
- Does the system provide continuous, automatic backups?
- Does the system have the capability to back up time-sensitive data like open files, emails, and databases?
- Does the system provide full coverage for complete data protection and recovery, including backup, offsite storage, ability to restore data over the network or dedicated storage device, online remote recovery, and offline archiving and recovery?
- Does the system provide instant file restores 24 hours a day, 7 days a week, 365 days a year?
- Does the system provide automatic notification of exceptions or problems encountered?
- Does the system provide detailed activity reports?
- Is the online data server in a geographic location that is separate from your locale?
- Does the online data storage provider take precautions for disasters in its own area, such as backing up on a server in another location?
- Is the online data storage provider's physical site secure? (The highest level of security is a Tier One Data Center Facility.)
- Is there a secure way for your firm to access the stored information, if someone loses the law firm encryption key?
- What access does the cloud service provider have to your data? Be sure to review the Terms of Service (TOS) or End User Licensing Agreement (EULA) or Service Level Agreement (SLA). Make no assumptions.
- Does the cloud service provider actually store your data, or is it stored elsewhere? Review any agreement between the cloud service provider and its data storage facility. Make no assumptions.

Online Data Storage:

- Carbonite
- CrashPlan
- FilesAnywhere
- Iron Mountain
- LiveVault
- Backblaze
- SpiderOak

See also, How to Back Up Your Computer, available online at https://www.osbplf.org/. (Select Practice Management, and then select Forms.)

NOTE: This information does not constitute an endorsement of or recommendation for a particular product or vendor. Technology changes over time. Attorneys should conduct their own appropriate research before using technology, and continue to review hardware and software over time. Attorneys who choose to use third-party online data storage should also review OSB Formal Opinion No. 2011-188.

ONLINE DATA STORAGE PROVIDERS

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund, except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices.
© 2019 OSB Professional Liability Fund

CHECKLIST FOR SCANNING CLIENT FILES

Imaging Client Files for Digital Storage

Before implementing a program to scan and digitally store client files, ask yourself: what kind of documents do you wish to store electronically and why? Do you want to scan closed client files with the intention of shredding the paper afterwards, or is the goal to go paperless from the start and eliminate or drastically reduce the need to maintain a physical file? In either case, consider the following:

1. If you are scanning closed files, are notes and memoranda included? By default, the client is entitled to attorney notes and memoranda unless exceptions apply. *See* OSB Formal Ethics Opinion No. 2017-192. The Professional Liability Fund (PLF) encourages lawyers to keep complete copies of their files.

2. If the goal is to go paperless from the outset, are *electronic* notes and memoranda preserved? *See* OSB Formal Ethics Opinion No. 2017-192.

3. Unsigned word processing documents are usually saved in their native format and stored in a subfolder for each client. How will you retain these documents once they are signed? There are several options:

   - Create a PDF from your word processing document and apply an authenticated digital signature. Retain the word processing document and the authenticated, signed PDF.
   - Create a PDF from your word processing document and use Adobe Acrobat's custom stamp tool to insert a scanned image of your signature. Retain the word processing document and the PDF with your scanned signature.
   - Create a jpeg of your scanned signature and insert it directly into your word processing document. Print the signed document to PDF. (Use File, Print to PDF so your signature is flattened.)
   - Keeping your word processing document intact, print a hard copy, sign it, scan it, and store it as a PDF.

   Note: See item 7 below for a discussion on saving documents in their native format. Also, note that you may elect to append the signed page to your original document when creating a PDF to store in your client file. See Adobe Acrobat Help for more information on creating and using authenticated digital signatures and custom stamps. If you intend to scan your signature and insert it into word processing or PDF documents, you will need image-editing software to crop the scanned signature and make the background transparent.

4. If imaged files are to be joined with documents that are electronic in origin, are all electronic document and database sources considered in the capture process? (Documents and databases residing on network servers, cloud servers, local hard drives, flash drives, disks, smartphones, or other media.)

5. Are documents being scanned at the lowest acceptable resolution and optimized afterwards to reduce file size? The resolution on most scanners can be adjusted quite easily. Adobe Acrobat has an optimization feature which helps further reduce file size after scanning.

6. Are scanned documents reviewed for quality and completeness of electronic capture?

7. Is the shelf life of the chosen electronic format acceptable? Saving digital file content using Adobe's archival standard (PDF/A) assures that *files created in earlier versions of Acrobat are*

guaranteed to be readable in future versions of PDF. This is not a given if you attempt to keep files in their native application (Microsoft® Word and WordPerfect® come to mind.) To learn more about the PDF/A format, see Reagan DeWitt-Henderson, "PDF/A – PDF for Archiving," *In Brief* (June 2011). Also, see the posts at The Acrolaw Blog, Acrobat for Legal Professionals. PDF /A is the preferred format for documents filed electronically with the courts.

8. Is your storage media up to the task? Storing scanned files on a hard drive or server that is properly backed up (see item 14 below) is preferable to using CDs or DVDs. Compact or digital video discs are made from layers of materials that can delaminate or oxidize over time. Environmental exposure, improper storage, or improper handling all present opportunities for this kind of media to degrade. To read more about this phenomena, see the article, "Protect Your CDs and DVDs," from the State Library & Archives of Florida.

9. Are imaged files electronically Bates-stamped or indexed? Organized in subfiles? Bates stamping, indexing, and organization of documents into subfiles will make it much easier to access needed information. Case management or document management software can make this process easier. Bates stamping can also be done in Adobe Acrobat.

10. Scanners are usually sold with OCR (optical character recognition) software. Without this technology, scanned documents are static images that cannot be searched. Is OCR software used as part of the scanning process to ensure that documents are searchable? If OCR software did not come packaged with your scanner, Adobe Acrobat has built-in text recognition capability. Search Help in Acrobat for step-by-step instructions on applying OCR during or after the scanning process. WordPerfect X6 and later also has built-in OCR capability. See Joe Kissell, "Building the Paperless Office" for an in-depth discussion of software, scanner settings, use of OCR technology, and more. The Acrolaw Blog also has helpful posts on using Acrobat for optical character recognition.

11. Are privileged litigation documents clearly marked in the electronic file?

12. Are documents not subject to client disclosure clearly marked in the electronic file? *See* Helen Hierschbiel, "Client Files, Revisited," *Oregon State Bar Bulletin* (June 2006), and OSB Formal Ethics Opinion No. 2017-192.

13. Are electronic files stored securely with password protection, encryption, or other security as needed? If you possess electronic data containing "consumer personal information" within the meaning of the Oregon Consumer Identity Theft Protection Act (ORS 646A.600 to 646A.628) you are required to develop, implement, and maintain safeguards to protect the security and disposal of the data. Failure to do so can result in civil penalties. For more information, see Kimi Nam, "Protect Client Information from Identity Theft," *In Brief*, (August 2008).

14. Are electronic files backed up daily (or more frequently)? Are backups stored on *and* off-site? Are the backups tested periodically? Are backups secured (password-protected, encrypted)? For a thorough discussion on backing up computer data and applications, see the PLF practice aid, *How to Backup Your Computer*.

15. Is an electronic file retention policy in place and enforced? Regardless of how files are retained, the PLF recommends that all client files be kept a minimum of 10 years. Some files may need to be kept longer. For more information, see the PLF practice aid, *File Retention and Destruction Guidelines*.

16. The lawyer responsible for a given matter should sign-off before electronic data is destroyed. Permanent destruction of electronic data requires special expertise. For more information, see the PLF practice aid, *File Retention and Destruction Guidelines*.

17. Scanning files can be expensive and time-consuming. Any odd-sized paper (legal size documents, phone message slips, post-it notes, fragile carbon copies, etc.) will require special handling. All paper clips and staples must be removed. Folded and hole-punched documents may jam the scanner. Be prepared to outsource or devote adequate staff time to major scanning projects. If you truly want to go paperless, or simply have less paper, start with active files or begin scanning files as you close them. Form good paper-processing habits, such as retaining client emails electronically rather than printing hard copies.

    For more information on retaining client emails, see the PLF practice aid, *Documenting Email as Part of the Client File*. Email archiving is easy with Adobe Acrobat 9 or later. *See* Beverly Michaelis, "Technology Tips – Using Acrobat 9 in the Law Office," *In Brief* (August 2008) and these posts at The Acrolaw Blog.

18. Is the firm aware of ethical considerations in going paperless? *See* Helen Hierschbiel, "Going Paperless," *Oregon State Bar Bulletin,* April 2009, and Amber Hollister, "Floating in the Cloud: The Ethics of Electronic Client Files," *Oregon State Bar Bulletin,* May 2017.

19. Is the firm aware of restrictions imposed by statute or rule that require retention of certain documents in original paper form? For more information, see the PLF practice aid, *File Retention and Destruction Guidelines*.

Disposition of Original Documents

1. Satisfy yourself that the imaging process has integrity (no missing or incomplete documents).

2. Communicate file retention policies to clients. Ideally, the issue of record retention should be addressed in the initial client fee agreement or engagement letter and again at the time of file closing. The PLF has sample fee agreement and engagement letters, as well as a sample closing letter, which incorporate file retention language. These practice aids are available at www.osbplf.org.

3. Review each file *individually*. Wholesale rules cannot apply due to discrepancies in file content. (See discussion below.)

4. Does the imaged file contain any client property? Documents, photographs, receipts, cancelled checks, or other materials provided by the client are generally considered *property* of the client and cannot be destroyed. However, this area requires judgment. It may be difficult to distinguish between one-of-a-kind original documents versus copies of documents provided by the client.

    Do your files contain client photographs? While it may be possible to scan and store a photograph as a high-quality digital image which can be printed at any time, the original nevertheless belongs to the client, is his/her property, and may be of special sentimental value.

    The PLF recommends that lawyers refrain from accepting original client property, or at a minimum, return client property at the time of file closing. For more information, see "Closing Files," a chapter in *A Guide to Setting Up and Running Your Law Office,* published by the PLF. The PLF also offers a File Closing Checklist. The book and the checklist are available at www.osbplf.org.

5. Does the file contain any original documents whose authenticity could be disputed? Documents that have particular legal importance? Documents that are enforceable or have value only in paper form? Examples include:

- Original Wills
- Original Powers of Attorney
- Original Directives to Physicians
- Deeds
- Car Titles
- Promissory Notes
- Contracts
- Fee Agreements (to pursue collection or defend yourself in a fee dispute)

Does your practice area require that you retain certain original documents? For example:

- Affidavit of Custodian – ORS 126.725(2).
- Original signed petitions, lists, schedules, statements, amendments, or electronic filing declarations in US Bankruptcy Court – Oregon LBR 5005-4(e).
- Documents that contain the original signature of a person other than the "filer" in Oregon eCourt must be retained for 30 days. UTCR 21.120 amended September 29, 2014 pursuant to Chief Justice Order 14-049.

This is not an exhaustive list. Conduct your own appropriate legal research and review files carefully. Know the rules and statutory requirements that apply to your practice area.

If you keep original wills, 40 years must elapse before the will can be disposed of. ORS 112.815 provides: "An attorney who has custody of a will may dispose of the will in accordance with ORS 112.820 if: (1) The attorney is licensed to practice law in the state of Oregon; (2) At least 40 years has elapsed since execution of the will; (3) The attorney does not know and after diligent inquiry cannot ascertain the address of the testator; and (4) The will is not subject to a contract to make a will or devise or not to revoke a will or devise."

6. File disposition must comply with applicable laws and the Oregon Rules of Professional Conduct. The Fair and Accurate Credit Transaction Act (FACTA) Disposal Rule (the Rule) requires any person who maintains or possesses "consumer information" for a business purpose to properly dispose of such information by taking "reasonable measures" to protect against unauthorized access to or use of the information in connection with its disposal. The Rule defines "consumer information" as any information about an individual that is in or derived from a consumer report. Although the Rule doesn't specifically refer to lawyers, it may be interpreted to apply to lawyers, and **the practices specified in the Rule would safeguard clients' confidential information.**

   "Reasonable measures" for disposal under the Rule are (1) burning, pulverizing, or shredding physical documents; (2) erasing or physically destroying electronic media; and (3) entering into a contract with a document disposal service. FACTA took effect June 1, 2005. Also, *see* OSB Formal Ethics Opinion No. 2005-141.

7. If your files contain personal health information, you must also comply with the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations. For more information, See Kelly T. Hagan, "Business Associate, Esq.: HIPAA's New Normal," *In Brief* (September 2013), and Kelly T. Hagan, "The HIPAA Compliance Process," *In Brief* (May 2014). Note: HIPAA rules also apply to PHI stored electronically.

8. When choosing a document or media disposal service, select a company certified by the National Association for Information Destruction (NAID). NAID members securely destroy materials in compliance with FACTA, HIPAA, and the Gramm-Leach-Bliley Acts. Casually discarded information is a risk and a liability.

9. The lawyer responsible for a given matter should sign off before the client's paper file is destroyed.

CHECKLIST FOR SCANNING CLIENT FILES

Resources

Professional Liability Fund
Review technology forms and *In Brief* articles available from the PLF, as well as CLE offerings. Visit the www.osbplf.org for more information.

American Bar Association
The ABA offers many print and online resources with an ongoing focus on technology, including the paperless office. These include *Law Practice* magazine, and the Legal Technology Resource Center. For an overview of resources, visit the ABA Law Practice Division.

Association for Records Management
ARMA International is a not-for-profit professional association and the authority on governing information as a strategic asset. ARMA International offers invaluable resources such as: legislative and regulatory updates; standards and best practices; technology trends and applications; live and web-based education; marketplace news and analysis; books & videos on managing records and information; and a global network of members.

National Association for Information Destruction
NAID is the international trade association for companies providing information destruction services. Suppliers of products, equipment, and services to destruction companies are also eligible for membership. NAID's mission is to promote the information destruction industry and the standards and ethics of its member companies. Locate a secure data destruction provider on the NAID website.

Acrobat for Legal Professionals
The Acrobat for Legal Professionals Blog is a resource for lawyers, law firms, paralegals, legal IT pros and anyone interested in the use of Acrobat in the legal community. Search the blog for helpful tips or videos on many topics, including scanning, OCR, and PDF/A for archiving.

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices. © 2019 OSB Professional Liability Fund.

COVID-19: Developing Protocols for Reopening Law Offices: Resources and Considerations

As Oregon lawyers begin thinking about reopening their law firms, there may be understandable confusion about when and how to do this. Neither the OSB nor the PLF can issue you a set of protocols for how you must handle this. We need to look to Governor Kate Brown's office for the proper directives and protocols. **The starting place is EXECUTIVE ORDER Number 20-12 issued by the Office of the Governor of the State of Oregon.**

Governor Brown has continued to stress there needs to be caution regarding our response to COVID-19. If law firms have been able to work remotely, they should continue to do so. If law firms have not been able to successfully work from home, they should follow their county's reopening guidelines.

Certain baseline criteria must be met before a specific county is eligible to apply for state approval to enter Phase 1 of reopening protocols while following health and safety guidelines. As of the date of this publication, not all counties have met the baseline criteria to apply for approval to enter Phase 1 reopening. After 21 days in Phase 1, counties continuing to meet the prerequisites may be able to enter Phase 2. The specifics for Phase 2 are still being worked out. It is important to get the most current mandates and guidelines regarding the state of Oregon's COVID-19 response. The State of Oregon website provides up-to-date information at Governor Kate Brown's "Building a Safe & Strong Oregon" home page where you can find COVID-19 Resources for Oregonians.

There are many sources of additional information that are helpful, especially from the Oregon Health Authority, the Centers for Disease Control and Prevention, and the World Health Organization. There are too many resources to list here. Below is just a sampling of the many good resources that are available.

1. Interim Guidance for Businesses and Employers Responding to Coronavirus Disease 2019 (COVID-19), May 2020 (CDC)

2. OSHA Guidance on Preparing Workplaces for COVID-19

3. Reopening Guidance – Cleaning and Disinfecting the Workplace (CDC)

4. COVID-19 Control and Prevention – OSHA

5. Retail Workers and Employers in Critical and High Customer-Volume Environments

6. COVID-19: Safety Tips for You – Red Cross

7. Office Safety Tips – National Safety Council

8. Getting Your Workplace Ready for COVID-19 (World Health Organization)

9. Coronavirus: Do's and Don'ts for Your Firm (ABA)

10. Cloth Face Coverings (CDC)

11. As States Move to Reopen, Law Firms Exercise Caution

12. Oregon Health Authority COVID-19 Updates

13. Oregon Health Authority Reopening Criteria

14. KATU News: Governor Brown Finalizes Phase 1 Guidelines for Reopening Oregon

15. MBA CLE: After the Quarantine: Employer Issues to Consider

16. ABA on-demand webinar: Preparing for Re-entry: The Most Important Takeaways from COVID-19 Quarantine

Please note: these resource links above are not represented as necessarily being the safest, best, or most current scientific, medical, or public health recommendations for office reopenings in the present COVID-19 environment. Similarly, they are not intended as legal advice regarding law-related issues concerning office reopenings. The links are simply examples of some of the informational resources available online at this time.