THE MODERN FILE CLERK: HOW TO DOCUMENT IN A PAPERLESS PRACTICE

CRISTAL ROBINSON, *Amarillo, TX*
Robinson Law, A CDR Law Group, PLLC

CAMERON BRUMFIELD, *Corpus Christi, TX*
Brumfield Law, PLLC

State Bar of Texas
__th ANNUAL
LAW PRACTICE MANAGEMENT
June 14, 2019
Austin, TX

CHAPTER 7

Cristal D. Robinson, JD MBA

3700 Red Fox Trail, Weddington, NC 28104|C: 704-497-1203 | cristal@cristalrobinson.com

LEGAL EXPERIENCE

Attorney	November 2008 - Current
Robinson Law (a CDR Law Group, PLLC firm)	Amarillo, TX
James Clark Law Firm, PLLC	Amarillo, TX
Whittenburg, Whittenburg, Stein, & Strange, PC	Amarillo, TX

EDUCATION

Master of Business Administration - West Texas A&M University; Canyon, TX	December 2009
Juris Doctor - Western Michigan University Cooley Law School; Lansing, MI	May 2007
Bachelor of Business Administration in Finance - West Texas A&M University; Canyon	August 2004

AWARDS, LEADERSHIP, AND MEMBERSHIP

Attorney Volunteer – Legal Aid of Northwest Texas
Legal Volunteer – Student Hurricane Network
Externship – Immigration Legal Services
Law Practice Management Committee – State Bar of TX
Committee Chair – Amarillo Women's Bar Association;
Founding Director – Collaborative Divorce of Amarillo
Education Task Force – Legal Aid of Northwest Texas
Executive Board Member – Panhandle Criminal Defense Law Association
Cabinet Member – United Way; Amarillo, TX
Public Interest Fellow – American Constitution Society
National Student Director – American Bar Association - Volunteer Income Tax – American Bar Assoc.
Professional Member – Charlotte LGBT Chamber of Commerce
Compliance Task Force & Host Parent – AFS
Mentor Program Chair – Rotary Club of Amarillo
Participant – Leadership Amarillo & Canyon
Chapter Director – Micro Investment Lending Institute®
Past President – Amarillo Women's Network
Writer and Producer – We the People, the Play; Amarillo, TX
Speaker – National Association of REALTORS
National Convention: Spoke to over 3000 people at *Superstar Panel* and *30 Under 30*
REALTOR Magazine: *30 Under 30* Article or *Energizing the Industry*

LICENSES

Texas – 24060505 11/2007
North Carolina – Application being processed

ADMITTED COURTS

United States District Court Northern District of Texas
Civil, Criminal, and Bankruptcy

CAMERON BRUMFIELD
Brumfield Law, PLLC
711 N. Carancahua St., Ste. 1825
Corpus Christi, TX 78401
Ph.: (361) 885-3804
Fax: (361) 885-0191
Cameron@BrumfieldLaw.com

BIOGRAPHICAL INFORMATION

EDUCATION

B.B.A. Management/Marketing, Texas Tech University Rawls College of Business
J.D. with Honors, Texas Tech University School of Law

PROFESSIONAL ACTIVIES

Sole Member, Brumfield Law, PLLC
Assistant County Attorney, Bee County, Texas
Member, Corpus Christi Bar Association
Member, Texas Bar College
Member, Law Practice Management Committee
Member, Bar Sections: Appellate Section, Business Law Section, Construction Law Section, Consumer and Commercial Law Section

COURTS OF ADMITTANCE

State of Texas, All courts
United States District Court – Southern District of Texas

PRACTICE AREAS

Child Protection Law
Construction Law
Consumer and Commercial Law
Business Law

SPEAKING ENGAGEMENTS AND PRESENTATIONS

Representing the Difficult Parent – CPS Attorney ad Litem Seminar, Corpus Christi TX – September 29, 2017

Table of Contents

I. Deciding to Move to a Paperless Practice

Today's law office relies heavily on technology and computers – it would be a strange sight to see an office without one. Computers allow attorneys to quickly draft and edit pleadings, forms, briefs, discovery, and other documents. Although still frequently tedious, compiling discovery is much easier and quicker. E-file has become mandatory. But attorneys often still heavily rely on print documents. For some attorneys, the habit or comfort of reading from a sheet of paper is difficult to give up, many attorneys still need print documents and hard copies, others continue to maintain a physical client file. However, in a 2015 survey by MyCase, 47% of survey respondents indicated they planned to move to a paperless practice.[1]

There are many benefits to moving to a paperless practice. First and foremost, it is worth noting that a "paperless practice" may be a misnomer – it doesn't necessarily mean your practice will use no paper. In fact, as mention above, there are still reasons why paper will remain an important part of our practices. Going paperless *does* mean reducing reliance on paper, creating digital storage and back-up systems, and utilizing technology to streamline your practice.

Perhaps the greatest advantage of a paperless practice is being able to access your files from anywhere with an internet connection. Once properly established, a user may connect to the firm's network through a secure connection called a virtual private network or VPN. Through the VPN, the user connects to the firm's network accesses the desired files. The user may open, view, download, and edit the files as desired. Of course, this can be done while connected to the network while in the office as well. This means an attorney or legal assistant can save a document or file to the network and another user can immediately access that file with nothing more than a few clicks of the mouse.

With the increase in portability and accessibility, the firm's productivity should increase. A properly establish paperless practice will have files and folders stored in a specific manner that makes finding

[1] https://www.lawtechnologytoday.org/2015/02/modernize-law-firms-2015/

and selecting the right file simple and quick – no more digging through file drawers to find the case you need and digging through papers to find a specific paragraph or paper. For text files, word searchable portable document format (PDF) documents allow for quickly locating specific words or phrases. Additionally, digital forms can be easily created to cut down on time while customizing a form to your needs. Reduced search times and ease of access add for increased productivity. Increased productivity leads to more profitability.

Profitability may also increase with a significant decrease in printing and copying costs. Not only will a firm save money for outsource printing and copying, but in-house copying and printing savings may be found. Because most firms already possess most, if not all, of the technology necessary to operate a paperless practice, the cost of converting is typically relatively low.

However, converting to a paperless practice is not without its downfalls. Some firms may not have much of the necessary technology that a paperless practice would require. This may include high performance scanners, network hubs and servers, back-up severs, and the necessary know-how of maintaining the firm's network. While many options exist for setting up a network and its back-ups, some options are more affordable than others. For example, a firm may want to utilize remote back-up for the firm's files. In such a set-up, the firm's server would connect to a dedicated off-site managed by a professional company. The advantage of having another company manage the firm's back-up server is the managing company provides all the necessary maintenance, hardware, and set-up. However, the advantages come with the increased costs associated with such advantages.

Converting to a paperless practice may also be difficult as attorney's often get set in their ways. The tradition and habit of having a hard file may be a hard one to break. Further, properly converting to a paperless practice requires careful planning, training, and in the event the firm converts all its hard files to digital, time. While a digital practice can be more secure, choosing and implementing the proper security protocols may present a challenge in and of itself. In that same realm, if the protocols and

methods for storing, managing, or modifying files and folders is not properly followed, information may be lost or destroyed.

Reasons to go Paperless	**Reasons not to go Paperless**
○ Practice Portability ○ State and Federal court documents already on the computer ○ Portability ○ Productivity ○ Practicality ○ Profitability	• Naming of Documents must be streamlined to find misplaced documents • Tradition • Time • Tooling • Training • Security • Expense

II. Applicable Ethics

A. Texas Disciplinary Rules of Professional Conduct Rule 1.01

Attorneys and their staff must be aware of relevant rules, cases, and ethics opinions in order to properly operate a paperless practice. Earlier this year, the Supreme Court of Texas amended paragraph 8 of the comment to rule 1.01 of the Texas Disciplinary Rules of Professional Conduct, stating that attorneys should "strive to become and remain proficient and competent in the practice of law, *including the benefits and risks associated with relevant technology.*"[2] Additionally, several opinions have been issued by the Professional Ethics Committee for the State Bar of Texas.

> Rule 1.01. Competent and Diligent Representation
>
> Maintaining Competence
>
> Comment 8. Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the

[2] Supreme Court of Texas Miscellaneous Docket Number 19-9016 "Order Amending Comment to the Texas Disciplinary Rules of Professional Conduct" Feb. 26, 2019.

> requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.

B. Professional Ethics Committee Opinion No. 648

One of the most common means of communicate in the present state of technology is through email. Some emails contain confidential or privileged information while others do not. The Texas Disciplinary Rules of Professional Conduct permit an attorney to use email to communicate confidential information by email.[3] The Professional Ethics Committee warns, however, that under some circumstances, a lawyer may have a duty to advise clients regarding risks incident to sending or receiving emails containing confidential information.[4] The attorney may further need to advise the client to consider using encrypted emails or another form of communication.[5]

C. Professional Ethics Committee Opinion No. 665

Attorneys must also take reasonable measures to prevent and avoid the transmission of confidential information embedded in electronic documents, including removing metadata before sending such documents to a person other than the lawyer's client.[6] "Reasonableness" will depend on the specific circumstances related to a specific incident or document.[7] Metadata is the data relating to data, but may include the author of a document, tags and categories (including geotags), who modified and document and when, and other such information.

---

[3] *See* Appendix A Ethics Opinion 648
[4] *Id.*
[5] *Id.*
[6] *See* Appendix B Ethics Opinion 665
[7] *Id.*

D. Professional Ethics Committee Opinion No. 680

While the Texas Disciplinary Rules of Professional Conduct do permit cloud-based data storage and back-up, attorneys must remain alert to the possibility of data breaches or disclosure of client confidential information.[8] Further, attorneys must undertake reasonable precautions in using cloud-based systems.[9] For attorneys who have access to or store protected health information, awareness and understand of the Health Information Portability and Accountability Act (HIPAA) as well as the Health Information Technology for Economic and Clinical Health (HITECH) which will be discussed further in this paper.

III. Data Storage and Protection

As a firm moves to a paperless practice, security and storage become a top priority. Anybody who uses computers for work knows one crash can devastate a practice and set an employee back days in work if not properly backed-up. Additionally, a data breach can be catastrophic, particularly when dealing with privileged or confidential information, such as protected health information[10] (PHI). With that in mind and in light of the applicable ethical, as well as statutory, rules, attorneys must take steps to protect and back-up that information.

A. HIPAA & HITECH

HIPAA provides strict penalties for any person who knowingly uses or causes to be used a unique health identifier, obtains PHI for an individual, or discloses PHI to another person.[11] In fact, the punishment ranges from a fine of not more than $50,000, imprisonment for not more than 1 year, or

---

[8] See Appendix C Ethics Opinion 680
[9] *Id.*
[10] Protected health information is any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment. It is sometimes called personal health information.
[11] 42 U.S.C. § 1320d-6

both, to up to a $250,000 fine, imprisonment for up to 10 years, or both.[12] Further, HITECH may have civil penalties of up to $1.5 million for violations of the act.[13] HITECH requires that covered entities[14] must obtain a business associate contract[15] with each covered entity or business associate providing for the compliance with applicable rules and regulations.[16] Further, in the event of a data breach[17], a covered entity will be required to notify each individual whose information may have been access, acquired, used, or disclosed.[18] The entity may also be required to notify media of such a breach, if the breach involves the PHI of more than 500 residents of a state or jurisdiction.[19]

B. Storage and Back-up

There are many options for data storage and protection that will provide the level of security a firm will require. However, every firm should have redundant storage and back-up to ensure stored data is not lost. The three most commonly used storage and back-up options include on-site storage, off-site storage, and cloud computing. As the name suggests, on-site storage is when the firm's server and back-up are stored at the same location as the firm. On-site storage is often cheaper than a dedicated off-site back-up server; however, on-site storage requires the firm to be responsible for the set-up and maintenance of the server. Off-site storage, on the other hand, could be in the form of cloud storage or a dedicated off-site server. The advantage of an off-site server is another person or entity is responsible for the maintenance and set-up of the server. Unfortunately, the maintenance comes with increase costs. Further, in the event of a catastrophe at a firm, such as fire, extreme weather, or physical break-in, on-site back-up may get damaged, destroyed, or stolen. On the other hand, off-site back-up alleviates those risks. Many small firms use cloud-based back-up solutions as they are cheap, easily implemented, and

---

[12] *Id.*
[13] 45 C.F.R. § 160.400 et seq.
[14] Defined in 45 C.F.R. 160.103.
[15] See Appendix D for a sample business associate contract or agreement.
[16] 45 U.S.C. § 164.105; 45 U.S.C. 160.103
[17] See Appendix E, A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)
[18] 45 C.F.R. § 164.404
[19] 45 C.F.R. § 164.406

can conform to the requirements of HIPAA and HITECH. Cloud-based back-up does not use a dedicated server but shares many of the benefits of off-site storage.

Determining which storage and back-up solution will depend largely on the particular needs and circumstances of the firm. However, every firm should be protecting its data through proper security measures. One of the most common security measures is encryption. Encryption is basically the scrambling of data for storage, then unscrambling that data when it is accessed or used. An encryption key is created that is used to access and unscramble the data. Varying levels and means of encryption exist, but one factor remains the same: encryption is only as strong as the key needed to access it. The most common form of a key is a password. Accordingly, the stronger the password, the stronger the protection. An additional down-side to encryption is the delay in the transmission of data. Because encryption scrambles and descrambles the data, computing power and time must be dedication to properly effectuating the encryption. For large files, such as video, picture, or large text files, encrypting the data may cause a slight slow-down in the transmission or access of the data. However, for most legal application, the decrease in speed may not even be noticed. Finally, because a key is necessary to accessing the encrypted data, losing the key may result in losing the data.

C. Encryption Pros and Cons

Pros	**Cons**
• Protects Data • Simple to implement • Common	• Slows down data transfer • Only as good as key • Lost key = lost data (usually)

D. Document Management Software (Cloud Storage)

Pros	**Cons**
• Can be accessed by using just an internet connection from anywhere. • Scalability of size of storage • Pay only for needed service amount • No data maintenance is required • Reliability of access	• Internet connections can slow down • Data security: Certain users may not feel comfortable having their valuable data stored on the cloud. This is because of the possibility that data can comingle with that of other organizations, as they are all stored remotely.

• Better communication between users • Access files through the web from any place, at any time, and on a wide variety of devices. • Less number of IT staff • Ease of use on device by storing onsite with using a logical drive • Effortless business modification as the company grows or moves	And, some may be concerned about the general privacy and security of the sensitive information stored in such remote facilities. • Requires encrypting data for security • Limitations on Bandwidth • Ongoing Costs

Feature	Box	Dropbox	Google Drive	MS OneDrive
Founded	2005	2007	2012	2007
Company Name	Box, Inc	Dropbox, Inc	Google	Microsoft
Focus	Larger Enterprise	Light Data	Teams	Windows Users
24/7 Customer Support	Yes	Yes	Yes	No
Business Version	Yes	Yes	No	Yes
Integration	Many	Many	Many	Many
Microsoft Office365	Yes	No	No	Yes, 1TB
Encryption				
PC Fetch Feature	Mirror files	Mirror Files	No	Yes
2-step Verification	Yes	Yes	No	No
OSes Supported	Windows, Mac, Android, iOS. Linux, Kindle	Windows, Mac, Android, iOS, Linux, Kindle	Windows, Mac, Android, iOS	Windows, Mac, Android, iOS, Kindle
Data Limit for Free	10 GB	2 GB	15 GB	5 GB
Price – Start Paid Plans	$10.00/ month – 100GB	$8.25/ month – 1TB	$2/ month - 100GB $10/month – 1TB	$2/ month - 50GB

IV. Tips for Utilizing a Paperless Office

Once your firmed has committed to a paperless office, properly implementing and utilizing technology, protocols, and policies should be carefully thought-out. First, the firm should decide on the particular hardware and technology to be used. Because files will be routinely scanned in, it is vital to have fast, efficient, and high-quality scanners. Additionally, firms should ensure that the monitors being utilized are large enough and provide for reduced eye strain. Utilizing dual monitors, at least 22” in size will greatly increase the efficiency and usability.

There are numerous programs and software that can be utilizing in a paperless practice, but few as useful as Adobe Acrobat Pro™. Although users can download Acrobat PDF viewers for free, the professional version of Acrobat offers functions that greatly increase the capabilities for a paperless firm. Specifically, Acrobat Pro allows for editing PDF files, creating fillable forms, bookmarks and nesting, converting documents to text searchable, e-signature, and removing metadata to name a few. Adobe offers training videos in order to fully take advantage of the full capabilities of Acrobat Pro. Most firms will already have a word processing program, such as Microsoft Word or Word Perfect. However, Acrobat Pro allows users to convert PDF files to Word files.

One of the primary benefits of a paperless practice is the ease and efficiency of locating files. However, to do so, a firm must establish uniform filing rules so that each document is readily found and easily identifiable. Consistency is the key to efficiency. An example of a filing system may include a folder for the client, with subfolders for each matter they are represented for, as well as general information such as completed intake forms. Files, such as pleadings, discovery, and motions should be saved using a uniform naming system such as "Orig.pet.1.1.2019" for an original petition drafted on January 1, 2019. Using abbreviations for the name of the file that match the name of the document make for easy identification. Dates allow for quick determination of whether it is the most up-to-date version of the document. Additionally, users may consider including their initials in the file name. The most important thing about creating the uniform filing system is for it to be simple, logical, and clear.

Many of the technologies and services that would be beneficial to a paperless practice can be found in a firm's practice management software. For example, many of the online platforms allow clients to access their files through the practice management portal, upload documents, pay bills, complete forms, and other useful systems. Additionally, some programs allow attorneys to share documents between firms, if so desired. Many programs have add-ins for email systems such as Microsoft Outlook™ or Gmail™, making saving emails to a client's folder simple and quick. It is important to browse the options and add-ins for each practice management system to determine which one allows the most

productivity specific to the firm's needs. It is equally important to continue training and education on the available services.

A. Client Management Software Cheat Sheets

Pros	**Cons**
• It puts everything you need into one place. • CRM is a scalable solution. • It allows for data mining. • The data being collected can be accessed remotely. • CRM can speed up the conversion process. • It lowers an organization's overall daily costs.	• It eliminates the human element from the business equation. • There can be security issues with CRM software. • Employees must go through a learning curve with the new system. • Technical support can be spotty • Data can still get lost if the database isn't properly maintained. • It can put sensitive data into the hands of a third party.

Feature	**Clio**	**Rocket Matter**	**MyCase**	**Practice Panther**
Founded	2008	2008	2010	2014
Company Name	Clio	Rocket Matter	AppFolio	Alpine Investors
Number of Employees	3500	30	1000	50
Security Audits	Regular 3rd party	Unknown	Unknown	Unknown
HIPAA Compliant	Not directly	Not stated	Not stated	Yes
Linkable time entries	Yes	Yes	Yes	Yes
Document Storage	Yes	Yes	Yes	Yes, Higher Fee
Flat Fee Billing	Yes	Yes	Yes	Yes, Higher Fee
API Access	Yes	Yes	No	Yes, Higher Fee
UTMBS Code billing	Yes	Yes	No	Yes, Higher Fee
Data Migration	Yes	Yes	No	Yes
Third-Party Integrations	125+	Around 11	<10	<20
QuickBooks	Yes	Yes	Yes	Yes
Outlook	Yes	Yes	Yes	Yes
Gmail	Yes	No	No	Yes
Google Calendar	Yes	Unknown	Yes	Yes
Dropbox	Yes	Yes	Yes	Yes
Box	Yes	Yes	No	Yes
OneDrive	Yes	No	No	Yes
Google Drive	Yes	No	No	No
Zapier	Yes	Yes	No	Yes
LawPay	Yes, included	No (Lexcharge)	No, another	Yes, included
Ruby Receptionist	Yes	Yes	No	Unknown
Website	Third Party	Third Party	Yes, Fee	Third Party
Uptime	99.9% guarantee	Unknown	Unknown	Online 99.9%
Support	24 hours a day	Global 24 hours	11 Hours	10 Hours a day
Self-Serve Support	6500+ articles	Unknown	<300 articles	<500 articles
Bar Partners	66 Bars	Unknown	35 Bars	16 Bars
Classrooms	150+	Unknown	Unknown	<10
Staff App	Yes	Yes	Yes	Yes

Client Portal App	No	No	No	No
Price	$39-99	$55 per user	$39	$39, 59, 79*

V. Electronic Communication

Technology has also established rapid means of communicating with clients, the court, opposing counsel, and other parties. Email, text messaging, instant messaging, and document clouds all have their unique benefits and pitfalls.

A. Email

Pros	**Cons**
• Sending an email to someone is very easy, people need little training to learn how to do this • Emails are free to send -so long as you have an email account and a connection to the Internet. • Emails are usually received fairly quickly, most of the time a couple of seconds after they are sent • People don't have to be present to receive the email • Emails can be sent any time of the day or night, 365 days a year • Files and images can be attached to an email • Multiple copies of a message can be sent to a group of people • A carbon copy of an email can be sent to other people • You can request proof of receipt or proof of the email being opened • Messages can be prepared in advance and saved until you are ready to send them. • Messages can be encrypted making it possible to send confidential information	• Both you and the person receiving the email must have an email address and access to a computer or device that can access the Internet • If you don't know the email address of the other person then you can't send them a message • Some people change their email addresses fairly often as they switch ISPs or jobs • Spam is a big problem, up to two-thirds of mails sent are spam • People can waste company time at work by sending emails to friends instead of working • When you are on holiday, your email box can become full and extra messages might not get stored • You may have to wait a long time to get a reply. • Email attachments can contain viruses • Some companies won't allow email attachments to be received • There are a lot of email scams and it is easy to get fooled by them

B. Text Messaging

Pros	**Cons**
• Can send them at any time, day or night • Person you are sending it to do not have to have their mobile phone switched on	• Only short messages can be sent • Needs nimble fingers to use some tiny mobile phone keypads • Needs basic typing skills

• Can save time sending a message rather than interrupting someone with a phone call • Good for informal messages • Good for helping friends and family keep in touch	• Can take some time to compile a message if you are not familiar with text speak shortcuts • Text speak spills over into written school work and formal communication • Should not be used for serious formal messages such as 'You are sacked.'

C. Instant Messaging – Facebook or AIM

Pros	**Cons**
• Allows you to chat in 'real time' to other people who also have an IM client • IM allows you to get on with other things and yet be in touch real time with connected friends and colleagues • Useful for customer support contact instead of having to phone a support line.	• As it is immediate, you have no time to reflect on the message you are sending, unlike an email where you can review the draft before sending. • In order to provide a free service, the IM providers send adverts and popup windows to each person. If you want to avoid this, you need to pay for a 'premium' service. • Unless you set up your IM client carefully, anyone can send you a message - not always a good thing.

D. Document Cloud – Adobe Document

Pros	**Cons**
• Very minimal hassle • This software integrates well with Acrobat. • It can save all your files into one cloud • Recipients can sign documents on phone • Recipients do not need special software or an account to complete forms and sign forms • Without changing the PDF format can edit and share the PDF file • Send files by email for signature • Can track signatures and views by recipient • Can print tracking for all views and changes • Shared cloud storage, multiple file formats, file conversion ability to sign documents • Ability to organize documents. able to change font across whole document • Able to split or merge PDF documents • It is a very efficient tool for searching and storing of digital files on Internet • Easy conversion of word document to pdf • Electronic signature is very efficient feature in this tool saves lot of time • It gives you a great flexibility in managing and organizations of PDF files. • All my editing and storing related problems are solved by this tool	• Must download products on multiple computers • Cost can get a little high per use • The Administrator cannot reset a user's password • Installation is bit complex for first time user • Installation speed is very slow • Cost is high as compared to other too • Web editor looks very primitive • It can be kind of slow sometimes • Pricing can get a little high make sure you only add users that are actively needing to you the product as you will be charged per user

VI. Conclusion

Although converting to a paperless practice may appear to be a daunting task, technology and information continues to make doing so easier with each day. Once operational, a paperless practice will enjoy increased productivity, portability, accessibility, and potentially profitability. It is important for firms to utilize up-to-date security and technological practices. Be sure to implement plans to prevent and respond to data breaches or losses. And finally, be sure to comply with all relevant ethical and statutory rules for digitally stored and managed information. Although this paper provides a starting point for converting, firms should be sure to thoroughly establish appropriate polices and seek assistance from knowledgeable professionals for information technology and managed services.

APPENDIX A

THE PROFESSIONAL ETHICS COMMITTEE
FOR THE STATE BAR OF TEXAS
Opinion No. 648

April 2015

QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

STATEMENT OF FACTS

Lawyers in a Texas law firm represent clients in family law, employment law, personal injury, and criminal law matters. When they started practicing law, the lawyers typically delivered written communication by facsimile or the U.S. Postal Service. Now, most of their written communication is delivered by web-based email, such as unencrypted Gmail.

Having read reports about email accounts being hacked and the National Security Agency obtaining email communications without a search warrant, the lawyers are concerned about whether it is proper for them to continue using email to communicate confidential information.

DISCUSSION

The Texas Disciplinary Rules of Professional Conduct do not specifically address the use of email in the practice of law, but they do provide for the protection of confidential information, defined broadly by Rule 1.05(a) to include both privileged and unprivileged client information, which might be transmitted by email.

Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:

> "a lawyer shall not knowingly:
> (1) Reveal confidential information of a client or former client to:
> (i) a person that the client has instructed is not to receive the information; or

> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."

A lawyer violates Rule 1.05 if the lawyer knowingly reveals confidential information to any person other than those persons who are permitted or required to receive the information under paragraphs (b), (c), (d), (e), or (f) of the Rule.

The Terminology section of the Rules states that "'[k]nowingly' . . . denotes actual knowledge of the fact in question" and that a "person's knowledge may be inferred from circumstances." A determination of whether a lawyer violates the Disciplinary Rules, as opposed to fiduciary obligations, the law, or best practices, by sending an email containing confidential information, requires a case-by-case evaluation of whether that lawyer knowingly revealed confidential information to a person who was not permitted to receive that information under Rule 1.05.

The concern about sending confidential information by email is the risk that an unauthorized person will gain access to the confidential information. While this Committee has not addressed the propriety of communicating confidential information by email, many other ethics committees have, concluding that, in general, and except in special circumstances, the use of email, including unencrypted email, is a proper method of communicating confidential information. See, e.g., ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof'l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008); Alaska Bar Ass'n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass'n Advisory Opinion on Prof'l Conduct, Op. 96-10 (1997); State Bar Ass'n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass'n, Advisory Ethics Op. No 97-05 (1997).

Those ethics opinions often make two points in support of the conclusion that email communication is proper. First, the risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Second, persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. See, e.g., Alaska Bar Ass'n Ethics Comm. Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998). The statute cited in those opinions is the Electronic Communication Privacy Act (ECPA), which makes it a crime to

intercept electronic communication, to use the contents of the intercepted email, or to disclose the contents of intercepted email. 18 U.S.C. § 2510 *et seq.* Importantly, the statute provides that "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." 18 U.S.C. § 2517(4).

The ethics opinions from other jurisdictions are instructive, as is Texas Professional Ethics Committee Opinion 572 (June 2006). The issue in Opinion 572 was whether a lawyer may, without the client's express consent, deliver the client's privileged information to a copy service hired by the lawyer to perform services in connection with the client's representation. Opinion 572 concluded that a lawyer may disclose privileged information to an independent contractor if the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information.

In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication. Examples of such circumstances are:

> 1. communicating highly sensitive or confidential information via email or unencrypted email connections;
> 2. sending an email to or from an account that the email sender or recipient shares with others;
> 3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));
> 4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
> 5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
> 6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

In the event circumstances such as those identified above are present, to prevent the unauthorized or inadvertent disclosure of confidential information, it may be appropriate for a lawyer to advise and caution a client as to the dangers inherent in sending or accessing emails from computers accessible to persons other than the client. A lawyer should also consider whether circumstances are present that would make it advisable to obtain the client's informed consent to the use of email communication, including the use of unencrypted email. See Texas Rule 1.03(b) and ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011). Additionally, a lawyer's evaluation of the lawyer's email technology and practices should be ongoing as there may be changes in the risk of interception of email communication over time that would indicate that certain or perhaps all communications should be sent by other means.

Under Rule 1.05, the issue in each case is whether a lawyer who sent an email containing confidential information knowingly revealed confidential information to a person who was not authorized to receive the information. The answer to that question depends on the facts of each case. Since a "knowing" disclosure can be based on actual knowledge or can be inferred, each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email.

This opinion discusses a lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct, but it does not address other issues such as a lawyer's fiduciary obligations or best practices with respect to email communications. Furthermore, it does not address a lawyer's obligations under various statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), which may impose other duties.

CONCLUSION

Under the Texas Disciplinary Rules of Professional Conduct, and considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication.

APPENDIX B

THE PROFESSIONAL ETHICS COMMITTEE
FOR THE STATE BAR OF TEXAS
Opinion No. 665

December 2016

QUESTIONS PRESENTED

1. What are a Texas lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct to prevent the inadvertent transmission of metadata containing a client's confidential information?

2. What are a Texas lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct when the lawyer receives from another lawyer a document that contains metadata that the receiving lawyer believes contains and inadvertently discloses confidential information of the other lawyer's client? For example, is the receiving lawyer permitted to search for, extract, and use the confidential information, and is the receiving lawyer required to notify the other lawyer of the receipt of the confidential information?

STATEMENT OF FACTS

Lawyer A represents a client in the settlement of a civil lawsuit. Lawyer A sends a draft settlement agreement to opposing counsel, Lawyer B, as an attachment to an email. The attachment includes embedded data, commonly called metadata. This metadata is digital data that is not immediately visible when the document is opened by the recipient of the email but can be read either through the use of certain commands available in word-processing software or through the use of specialized software. In this case, the metadata includes information revealing confidential information of the client of Lawyer A related to ongoing settlement negotiations. Lawyer B has no reason to believe that Lawyer A intended to include this metadata in the attachment.

DISCUSSION

In this opinion, "confidential information" refers to both privileged information and unprivileged client information, as defined in Rule 1.05(a) of the Texas Disciplinary Rules of Professional Conduct.

The exchange of electronic documents is an essential part of modern law practice. When an electronic document is created or edited, some computer programs will automatically embed information in the document. Embedded information that describes the history, tracking, or management of an electronic document is commonly known as "metadata." A common example of metadata is embedded information that describes the identity of the owner of the computer that created the document and the date and time of creation. Similarly, some computer programs use

embedded metadata to track the changes made to a document as well as the comments of the various reviewers of the document.

Frequently the exchange of metadata between lawyers is either mutually beneficial or otherwise harmless, such as when a lawyer intentionally transmits a document containing tracked changes in order to facilitate the negotiating process. However, the inadvertent disclosure of metadata containing a client's confidential information could be harmful to the client. The risk of such inadvertent disclosure is heightened by the fact that metadata is generally not visible from the face of an electronic document unless the user takes some additional action.

The first question raised is whether the Texas Disciplinary Rules of Professional Conduct require lawyers to take steps to prevent the inadvertent transmission of metadata containing confidential information. The answer is governed by Rules 1.01 and 1.05.

With certain exceptions not relevant here, Rule 1.01 generally prohibits a lawyer from accepting or continuing "employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence." "Competence," as defined by the Terminology Section of the Texas Disciplinary Rules, "denotes possession or the ability to timely acquire the legal knowledge, skill, and training reasonably necessary for the representation of the client."

Rule 1.05 generally prohibits lawyers from knowingly revealing confidential information to a lawyer representing the opposing party, subject to limited exceptions set out in the Rule. Rule 1.05 reflects a lawyer's duty "to maintain confidentiality of information acquired by the lawyer during the course of or by reason of the representation of the client." Comment 2 to Rule 1.05. "Knowingly," as used in Rule 1.05, "denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances." Terminology Section of the Texas Disciplinary Rules.

In the opinion of the Committee, a lawyer's duty of competence requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that the transmitted metadata may include confidential information, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata. Lawyers therefore have a duty to take reasonable measures to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons to whom such confidential information is not to be revealed pursuant to the provisions of Rule 1.05. Commonly employed methods for avoiding the disclosure of confidential information in metadata include the use of software to remove or "scrub" metadata from the document before transmission, the conversion of the document into another format that does not preserve the original metadata, and transmission of the document by fax or hard copy.

Whether a lawyer has taken reasonable measures to avoid the disclosure of confidential information in metadata will depend on the factual circumstances. Relevant factors in determining reasonableness include the steps taken by the lawyer to prevent the disclosure of the confidential information in metadata, the sensitivity of the metadata revealed, the identity of the intended

recipient, and other considerations appropriate to the facts. Not every inadvertent disclosure of confidential information in metadata will violate Rule 1.05.

The second question is whether the Texas Disciplinary Rules impose particular duties on a lawyer who receives an electronic document containing metadata that appears to include confidential information of another party. There is no specific provision in the Texas Disciplinary Rules requiring a lawyer to take or refrain from taking any particular action in such a situation. *See* Professional Ethics Committee Opinion 664 (October 2016) ("The Texas Disciplinary Rules of Professional Conduct do not prescribe a specific course of conduct a lawyer must follow upon the unauthorized or inadvertent receipt of another party's confidential information outside the normal course of discovery.").

In the absence of specific provisions of the Texas Disciplinary Rules governing this situation, the Committee can offer only limited guidance for lawyers dealing with the receipt of documents containing metadata. In most circumstances, the provisions of the Texas Disciplinary Rules that must be considered by lawyers with respect to the receipt of documents containing metadata are Rule 8.04(a)(3), which requires that a lawyer shall not "engage in conduct involving dishonesty, fraud, deceit or misrepresentation," and Rule 3.03(a)(1), which requires that a lawyer shall not knowingly "make a false statement of material fact or law to a tribunal." Thus, although the Texas Disciplinary Rules do not prohibit a lawyer from searching for, extracting, or using metadata and do not require a lawyer to notify any person concerning metadata obtained from a document received, a lawyer who has reviewed metadata must not, through action or inaction, convey to any person or adjudicative body information that is misleading or false because the information conveyed does not take into account what the lawyer has learned from such metadata. For example, a Texas lawyer, in responding to a question, is not permitted to give an answer that would be truthful in the absence of metadata reviewed by the lawyer but that would be false or misleading when the lawyer's knowledge gained from the metadata is also considered.

The Committee notes that professional ethics standards in some other jurisdictions include specific requirements applicable to this situation. These specific requirements vary from state to state and may include a requirement to notify the sender of a document believed to contain inadvertently sent metadata and a requirement not to search for or read such metadata. For example, a number of jurisdictions have adopted part or all of the approach used in the current version of Rule 4.4(b) of the American Bar Association Model Rules of Professional Conduct, which provides:

> "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."

To the extent a Texas lawyer becomes subject to the disciplinary rules of other jurisdictions, the lawyer may be subject to additional requirements concerning the treatment of metadata that would not be applicable if only the Texas Disciplinary Rules of Professional Conduct were considered.

The Committee also cautions that a lawyer's conduct upon receipt of an opponent's confidential information may have material consequences for the client, including the possibility of procedural disqualification. *See In re Meador*, 968 S.W.2d 346, 351-52 (Tex. 1998) (in a case not involving metadata, discussing factors to be considered in deciding whether to disqualify counsel who received the opposing party's privileged information outside of discovery, including the promptness with which the lawyer notified the opposing counsel of the circumstances). If in a given situation a client will be exposed to material risk by a lawyer's intended treatment of an opponent's inadvertently transmitted confidential information contained in metadata, the lawyer should discuss with the client the risks and benefits of the proposed course of action as well as other possible alternatives so that the client can make an informed decision. *See* Rule 1.03(b) ("A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.").

This opinion applies only to the voluntary transmission of electronic documents outside the normal course of discovery. The production of electronic documents in discovery is governed by court rules and other law, which may prohibit the removal or alteration of metadata. Court rules may also govern the obligations of a lawyer who receives inadvertently transmitted privileged information in the course of discovery. *See, e.g.*, Tex. R. Civ. P. 193.3(d).

CONCLUSION

The Texas Disciplinary Rules of Professional Conduct require lawyers to take reasonable measures to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons other than the lawyer's client. Whether a lawyer has taken reasonable measures to avoid the disclosure of confidential information in metadata will depend on the factual circumstances.

While the Texas Disciplinary Rules of Professional Conduct do not prescribe a specific course of conduct for a lawyer who receives from another lawyer an electronic document containing confidential information in metadata that the receiving lawyer believes was not intended to be transmitted to the lawyer, court rules or other applicable rules of conduct may contain requirements that apply in particular situations. Regardless, a Texas lawyer is required by the Texas Disciplinary Rules to avoid misleading or fraudulent use of information the lawyer may obtain from the metadata. In the absence of specific governing provisions, a lawyer who is considering the proper course of action regarding confidential information in metadata contained in a document transmitted by opposing counsel should determine whether the possible course of action poses material risks to the lawyer's client. If so, the lawyer should explain the risks and potential benefits to the extent reasonably necessary to permit the client to make informed decisions regarding the matter.

APPENDIX C

THE PROFESSIONAL ETHICS COMMITTEE
FOR THE STATE BAR OF TEXAS
OPINION NO. 680

September 2018

QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct may a lawyer use cloud-based client data storage systems or use cloud-based software systems for the creation of client-specific documents where confidential client information is stored or submitted to a cloud-based system?

STATEMENT OF FACTS

A lawyer is considering subscribing to various cloud-based electronic storage and software systems that allow users to store confidential client information or prepare form legal documents by uploading confidential client information for insertion into those form documents. The lawyer is concerned because these cloud-based electronic storage and software systems are owned by private companies, the various computer servers on which this client confidential information would reside are or may be located in other countries, the client information could be accessed by employees of these private companies, and there is the possibility of these servers and the confidential information residing on them being "hacked" by third parties or being rendered inaccessible as a result of a cloud storage vendor going out of business. The lawyer questions whether it is ethical to use cloud-based electronic storage or software systems given these conditions and the potential disclosure risks to confidential client information.

DISCUSSION

Rule 1.05(a) of the Texas Disciplinary Rules of Professional Conduct broadly defines client "confidential information" as including both "privileged information" and "unprivileged client information." The latter means "all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client." Rule 1.05(a).

Rule 1.05(b) provides in part that, "[e]xcept as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly:

(1) Reveal confidential information of a client or former client to:

(i) a person that the client has instructed is not to receive the information; or

> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."

A lawyer violates Rule 1.05 if the lawyer knowingly reveals confidential information to any person other than those persons who are permitted or required to receive the information under paragraphs (b), (c), (d), (e), or (f) of the Rule. The Terminology section of the Rules states that "'[k]nowingly' . . . denotes actual knowledge of the fact in question" and that a "person's knowledge may be inferred from circumstances."

Professional Ethics Opinion 648 (April 2015) addressed the question of whether a lawyer could ethically transmit client confidential information by email. The Committee concluded that, "considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication." Similarly, Opinion 572 (June 2006) determined that, "[u]nder the Texas Disciplinary Rules of Professional Conduct, unless the client has instructed otherwise, a lawyer may deliver materials containing privileged information to an independent contractor, such as a copy service, hired by the lawyer in the furtherance of the lawyer's representation of the client if the lawyer reasonably expects that the confidential character of the information will be respected by the independent contractor."

Cloud-based electronic storage and software systems are in wide use among the general public and lawyers. While wide usage of an information storage method or software document creation system is not, in itself, justification for its use by lawyers, alternative methods of information storage and document preparation also have an inherent risk of disclosure or misuse—just as a privileged letter to a client through the U.S. Postal Service (versus transmission through email) can be intercepted or accessed by third parties and a client's file in a lawyer's office may be susceptible to access or disclosure by unauthorized parties without the lawyer "knowingly" revealing that information.

Considering the present state of technology, its common usage to store confidential information, and the potential cost and time savings for clients, a lawyer may use cloud-based electronic data systems and document preparation software for client confidential information; however, lawyers should remain continually alert to the vulnerability of cloud-based vendors and systems to data breaches and whether a particular vendor or system appears to be unusually vulnerable, based on systemic failures by that vendor or system of which the lawyer should be aware. In certain circumstances, a lawyer may decide that some client confidential information is too vulnerable to unauthorized access or disclosure to risk its storage or use in a cloud-based electronic system or too vulnerable to such risk without that data being adequately encrypted or without additional technological safeguards in place. Data "hacking" by third parties is becoming increasingly well-known and can even occur with respect to client confidential information

stored on a server within a law firm. Therefore, a lawyer should remain reasonably aware of changes in technology and the associated risks—without unnecessarily retreating from the use of new technology that may save significant time and money for clients. In some circumstances it may be appropriate to confer with a client regarding these risks as applicable to a particular matter and obtain a client's input regarding or consent to using cloud-based electronic data systems and document preparation software. Of course, if a client has given specific instructions regarding the use and protection of its client confidential information in a matter those instructions must be followed except when otherwise required or permitted by the provisions of Rule 1.05.

Still, a lawyer must take reasonable precautions in the adoption and use of cloud-based technology for client document and data storage or the creation of client-specific documents that require client confidential information. These reasonable precautions include: (1) acquiring a general understanding of how the cloud technology works; (2) reviewing the "terms of service" to which the lawyer submits when using a specific cloud-based provider just as the lawyer should do when choosing and supervising other types of service providers; (3) learning what protections already exist within the technology for data security; (4) determining whether additional steps, including but not limited to the encryption of client confidential information, should be taken before submitting that client information to a cloud-based system; (5) remaining alert as to whether a particular cloud-based provider is known to be deficient in its data security measures or is or has been unusually vulnerable to "hacking" of stored information; and (6) training for lawyers and staff regarding appropriate protections and considerations. These precautions do not require lawyers to become experts in technology; however, they do require lawyers to become and remain vigilant about data security issues from the outset of using a particular technology in connection with client confidential information. The Committee refrains from setting out specific requirements for assessing reasonableness since some precautions become obsolete over time with changing technologies and the risks may change as well.

Rule 1.01(a) requires that lawyers exhibit "competence" in representing clients. In Opinion 665 (December 2016), the Committee applied Rule 1.01 to a question involving a lawyer's inadvertent transmission to third parties of electronic metadata within client documents and concluded that the Rule's "competency" requirement was applicable to a lawyer's technological competence in preserving client confidential information. The Committee reiterates here the necessity of competence by lawyers and their staff regarding data protection considerations of cloud-based systems.

CONCLUSION

Under the Texas Disciplinary Rules of Professional Conduct, a lawyer may use a cloud-based electronic data storage system or cloud-based software document preparation system to store client confidential information or prepare legal documents. However, lawyers must remain alert to the possibility of data breaches, unauthorized access, or disclosure of client confidential information and undertake reasonable precautions in using those cloud-based systems.

APPENDIX D

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:

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;

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;

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;

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

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.

APPENDIX E

My entity just experienced a cyber-attack! What do we do now?

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

Has your entity just experienced a ransomware attack or other cyber-related security incident,[i] and you are wondering what to do now? This guide explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In the event of a cyber-attack or similar emergency an entity:

- Must execute its response and mitigation procedures and contingency plans.[ii] For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of protected health information,[iii] which may be done by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate,[iv] if it has access to protected health information for that purpose).

- Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule.[v] If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.[vi]

- Should report all cyber threat indicators[vii] to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. OCR does not receive such reports from its federal or HHS partners.[viii]

- Must report the breach[ix] to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify: individuals

without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

OCR considers all mitigation efforts taken by the entity during in any particular breach investigation.[x] Such efforts include voluntary sharing of breach-related information with law enforcement agencies and other federal and analysis organizations as described above.[xi]

---

[i] The HIPAA Security Rule defines a "security incident" as the attempted or successful unauthorized access, use, disclosure, modification, or destructions of information or interference with system operations in an information system. See 45 C.F.R. § 164.304. For additional details on OCR's recommendations for preventing and responding to a ransomware attack, please refer to OCR's ransomware guidance. See https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[ii] The HIPAA Security Rule requires HIPAA covered entities and business associate to identify and respond to suspect or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. See 45 C.F.R. § 164.308(a)(6). The HIPAA Security Rule also requires HIPAA covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans, and emergency mode operation plans. See 45 C.F.R. § 164.308(a)(7). See also https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es.

[iii] Protected health information or PHI includes all individually-identifiable health information held by HIPAA covered entities and business associate, except for employment records, records covered by FERPA, or information about individuals deceased more than 50 years. PHI includes any health information that relates to the care or payment for care for an individual, and includes, for example, treatment information, billing information, insurance information, contact information, and social security numbers. See also https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[iv] A business associate includes any vendor that creates, receives, maintains, or transmits protected health information (PHI) for or on behalf of a HIPAA covered entity. This includes vendors that have access to PHI to provide IT-related services to the covered entity. See 45 C.F.R. § 164.103, § 164.308, and § 164.502. See also https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[v] The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

[vi] See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.412.

[vii] The Cybersecurity Information Sharing Act of 2015 (CISA) describes cyber threat indicators as information that is necessary to describe or identify: malicious reconnaissance; methods of defeating a security control or exploitation of a security vulnerability; a security vulnerability; methods of causing a user with legitimate access to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; a description of actual or potential harm caused by an incident; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination thereof. See also https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/index.html.

[viii] The Cybersecurity Information Sharing Act of 2015 (CISA) in Sec. 106 provides that "liability protections are provided to entities acting in accordance with this title that: (1) monitor information systems; or (2) share or receive indicators or defensive measures, provided that the manner in which an entity shares such indicators or measures with the federal government is consistent with specified procedures and exceptions set forth under the DHS sharing process."

[ix] Breaches affecting fewer than 500 individuals should be reported to affected individuals as soon as possible, but within no later than 60 days, and reported to OCR within 60 days of the end of the calendar year in which the breach was discovered. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.404 and 164.408.
See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.402-414.

[x] The HIPAA Enforcement Rule includes provides that in determining the amount of any applicable civil money penalty, OCR may consider mitigating factors, including matters that justice may require. See 45 C.F.R. § 160.408(e). See also https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html.

[xi] The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

APPENDIX F

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download.

[2] Exfiltration is "[t]he unauthorized transfer of information from an information system." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

- training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
- implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

The Security Management Process standard of the Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ***all*** of the ePHI the entities create, receive, maintain, or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. It is expected that covered entities and business associates will use this process of risk analysis and risk management not only to satisfy the specific standards and implementation specifications of the Security Rule, but also when implementing security measures to reduce the particular risks and vulnerabilities to ePHI throughout an organization's entire enterprise, identified as a result of an accurate and thorough risk analysis, to a reasonable and appropriate level. For example, although there is a not a Security Rule standard or implementation specification that specifically and expressly requires entities to update the firmware[3] of network devices, entities, as part of their risk analysis and risk management process, should, as appropriate, identify and address the risks to ePHI of using networks devices running on obsolete firmware, especially when firmware updates are available to remediate known security vulnerabilities.

In general, moreover, the Security Rule simply establishes a floor, or minimum requirements, for the security of ePHI; entities are permitted (and encouraged) to implement additional and/or more stringent security measures above what they determine to be required by Security Rule standards.

3. Can HIPAA compliance help covered entities and business associates recover from infections of malware, including ransomware?

Yes. The HIPAA Security Rule requires covered entities and business associates to implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack.

Because ransomware denies access to data, maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Because some ransomware variants have been known to remove or otherwise disrupt online backups, entities should consider maintaining backups offline and unavailable from their networks.

[3] Firmware refers to "[c]omputer programs and data stored in hardware… such that the programs and data cannot be dynamically written or modified during execution of the programs." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013).
Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Implementing a data backup plan is a Security Rule requirement for HIPAA covered entities and business associates as part of maintaining an overall contingency plan. Additional activities that must be included as part of an entity's contingency plan include: disaster recovery planning, emergency operations planning, analyzing the criticality of applications and data to ensure all necessary applications and data are accounted for, and periodic testing of contingency plans to ensure organizational readiness to execute such plans and provide confidence they will be effective. See 45 C.F.R. 164.308(a)(7).

During the course of responding to a ransomware attack, an entity may find it necessary to activate its contingency or business continuity plans. Once activated, an entity will be able to continue its business operations while continuing to respond to and recover from a ransomware attack. Maintaining confidence in contingency plans and data recovery is critical for effective incident response, whether the incident is a ransomware attack or fire or natural disaster.

Security incident procedures, including procedures for responding to and reporting security incidents, are also required by HIPAA. See 45 C.F.R. 164.308(a)(6). An entity's security incident procedures should prepare it to respond to various types of security incidents, including ransomware attacks. Robust security incident procedures for responding to a ransomware attack should include processes to[4]:

- detect and conduct an initial analysis of the ransomware;
- contain the impact and propagation of the ransomware;
- eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

4. How can covered entities or business associates detect if their computer systems are infected with ransomware?

Unless ransomware is detected and propagation halted by an entity's malicious software protection or other security measures, an entity would typically be alerted to the presence of ransomware only after the ransomware has encrypted the user's data and alerted the user to its presence to demand payment. However, in some cases, an entity's workforce may notice early indications of a ransomware attack that has evaded the entity's security measures. HIPAA's requirement that an entity's workforce receive appropriate security training, including training for detecting and reporting instances of malicious

[4] Adapted from NIST SP 800-61Rev. 2, *Computer Security Incident Handling Guide.*

software, can thus assist entities in preparing their staff to detect and respond to ransomware. Indicators of a ransomware attack could include:

- a user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature;
- an increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- an inability to access certain files as the ransomware encrypts, deletes and re-names and/or re-locates data; and
- detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

If an entity believes that a ransomware attack is underway, either because of indicators similar to those above or other methods of detection, the entity should immediately activate its security incident response plan, which should include measures to isolate the infected computer systems in order to halt propagation of the attack.

Additionally, it is recommended that an entity infected with ransomware contact its local FBI or United States Secret Service field office. These agencies work with Federal, state, local and international partners to pursue cyber criminals globally and assist victims of cybercrime.

5. What should covered entities or business associates do if their computer systems are infected with ransomware?

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R. 164.308(a)(6).

HIPAA covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that they believe are reasonable and appropriate to respond to malware and other security incidents, including ransomware attacks. Entities seeking guidance regarding the implementation of security incident procedures may wish to review NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*[5] for additional information.

An entity's security incident response activities should begin with an initial analysis to:

[5] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- determine the scope of the incident to identify what networks, systems, or applications are affected;
- determine the origination of the incident (who/what/where/when);
- determine whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and
- determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).

These initial steps should assist the entity in prioritizing subsequent incident response activities and serve as a foundation for conducting a deeper analysis of the incident and its impact. Subsequent security incident response activities should include steps to:

- contain the impact and propagation of the ransomware;
- eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

Part of a deeper analysis should involve assessing whether or not there was a breach of PHI as a result of the security incident. The presence of ransomware (or any malware) is a security incident under HIPAA that may also result in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack. See the definition of disclosure at 45 C.F.R. 160.103 and the definition of breach at 45 C.F.R. 164.402.

6. Is it a HIPAA breach if ransomware infects a covered entity's or business associate's computer system?

Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.[6]

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized

[6] See also Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

7. How can covered entities or business associates demonstrate "…that there is a low probability that the PHI has been compromised" such that breach notification would not be required?

To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. the unauthorized person who used the PHI or to whom the disclosure was made;

3. whether the PHI was actually acquired or viewed; and

4. the extent to which the risk to the PHI has been mitigated.

A thorough and accurate evaluation of the evidence acquired and analyzed as a result of security incident response activities could help entities with the risk assessment process above by revealing, for example: the exact type and variant of malware discovered; the algorithmic steps undertaken by the malware; communications, including exfiltration attempts between the malware and attackers' command and control servers; and whether or not the malware propagated to other systems, potentially affecting additional sources of electronic PHI (ePHI). Correctly identifying the malware involved can assist an entity to determine what algorithmic steps the malware is programmed to perform. Understanding what a particular strain of malware is programmed to do can help determine how or if a particular malware variant may laterally propagate throughout an entity's enterprise, what types of data the malware is searching for, whether or not the malware may attempt to exfiltrate data, or whether or not the malware deposits hidden malicious software or exploits vulnerabilities to provide future unauthorized access, among other factors.

Although entities are required to consider the four factors listed above in conducting their risk assessments to determine whether there is a low probability of compromise of the ePHI, entities are encouraged to consider additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised. If, for example, there is high risk of unavailability of the data, or high risk to the

integrity of the data, such additional factors may indicate compromise. In those cases, entities must provide notification to individuals without unreasonable delay, particularly given that any delay may impact healthcare service and patient safety.

Additionally, with respect to considering the extent to which the risk to PHI has been mitigated (the fourth factor) where ransomware has accessed PHI, the entity may wish to consider the impact of the ransomware on the integrity of the PHI. Frequently, ransomware, after encrypting the data it was seeking, deletes the original data and leaves only the data in encrypted form. An entity may be able to show mitigation of the impact of a ransomware attack affecting the integrity of PHI through the implementation of robust contingency plans including disaster recovery and data backup plans. Conducting frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack and ensuring the integrity of PHI affected by ransomware. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Integrity to PHI data is only one aspect when considering to what extent the risk to PHI has been mitigated. Additional aspects, including whether or not PHI has been exfiltrated, should also be considered when determining the extent to which the risk to PHI has been mitigated.

The risk assessment to determine whether there is a low probability of compromise of the PHI must be thorough, completed in good faith and reach conclusions that are reasonable given the circumstances. Furthermore, in accordance with 45 C.F.R. 164.530(j)(iv)), covered entities and business associates must maintain supporting documentation sufficient to meet their burden of proof (see 45 C.F.R. 164.414) regarding the breach assessment – and if applicable, notification - process including:

- documentation of the risk assessment demonstrating the conclusions reached;
- documentation of any exceptions determined to be applicable to the impermissible use or disclosure (see 45 C.F.R. 164.402(1)) of the PHI; and
- documentation demonstrating that all notifications were made, if a determination was made that the impermissible use or disclosure was a reportable breach.

8. Is it a reportable breach if the ePHI encrypted by the ransomware was already encrypted to comply with HIPAA?

This is a fact specific determination. The HIPAA breach notification provisions apply to "unsecured PHI" (see 45 C.F.R. 164.402), which is protected health information (PHI) that is not secured through the use of a technology or methodology specified by the Secretary in guidance. If the electronic PHI (ePHI) is encrypted by the entity in a manner consistent with the *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*[7] such that it is no longer "unsecured PHI," then the entity is not required to conduct a risk assessment to determine if there is a low probability of compromise, and breach notification is not required.

[7] Available at http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

However, even if the PHI is encrypted in accordance with the HHS guidance, additional analysis may still be required to ensure that the encryption solution, as implemented, has rendered the affected PHI unreadable, unusable and indecipherable to unauthorized persons. A full disk encryption solution may render the data on a computer system's hard drive unreadable, unusable and indecipherable to unauthorized persons while the computer system (such as a laptop) is powered down. Once the computer system is powered on and the operating system is loaded, however, many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user.

For example, if a laptop encrypted with a full disk encryption solution in a manner consistent with HHS guidance[8] is properly shut down and powered off and then lost or stolen, the data on the laptop would be unreadable, unusable and indecipherable to anyone other than the authenticated user. Because the PHI on the laptop is not "unsecured PHI", a covered entity or business associate need not perform a risk assessment to determine a low probability of compromise or provide breach notification.

However, in contrast to the above example, if the laptop is powered on and in use by an authenticated user, who then performs an action (clicks on a link to a malicious website, opens an attachment from a phishing email, etc.) that infects the laptop with ransomware, there could be a breach of PHI. If full disk encryption is the only encryption solution in use to protect the PHI and if the ransomware accesses the file containing the PHI, the file containing the PHI will be transparently decrypted by the full disk encryption solution and access permitted with the same access levels granted to the user.

Because the file containing the PHI was decrypted and thus "unsecured PHI" at the point in time that the ransomware accessed the file, an impermissible disclosure of PHI was made and a breach is presumed. Under the HIPAA Breach Notification Rule, notification in accordance with 45 CFR 164.404 is required unless the entity can demonstrate a low probability of compromise of the PHI based on the four factor risk assessment (see 45 C.F.R. 164.402(2)).

[8] HHS guidance to render unsecured PHI unusable, unreadable or indecipherable to unauthorized individuals indicates that encryption solutions for data-at-rest must be consistent with NISP SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, in order for encrypted PHI to not be "unsecured PHI". It must be noted, however, that consistency with NIST SP 800-111 requires not only the consideration of an encryption algorithm, but also consideration of additional areas of an encryption solution including encryption methodologies (e.g., full disk, virtual disk/volume, folder/file), cryptographic key management, and pre-boot authentication, where applicable.

The Modern File Clerk: How to Document

Cameron Brumfield, Corpus Christi - Brumfield Law, PLLC

Cristal Robinson, Amarillo - Robinson Law, A CDR Law Group, PLLC

June 14, 2019
2:00 PM

SBOT CLE: .5 hours

Rule 1.01. Competent and Diligent Representation

Maintaining Competence

8. Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.

IN THE SUPREME COURT OF TEXAS - Misc. Docket No. 19-9016 Dated: Feb. 26, 2019

Ethics Opinions

- **Ethics Opinion 648:**
  - Lawyer May communicate by email, generally
  - May require advice to client of danger
- **Ethics Opinion 665:**
  - Lawyer must take reasonable steps to prevent transmission of confidential information in electronic data
  - Remove metadata
- **Ethics Opinion 680:**
  - Cloud-based electronic data storage permitted
  - Remain alert to security threats

Considerations in Going Paperless

PROS

- Portability
- Productivity
- Practicality
- Profitability

CONS

- Tradition
- Time
- Tooling
- Training
- Security
- Expense

Federal Regulations

HIPAA

- "Health Insurance Portability and Accountability Act"
- 42 U.S.C. § 1320d-6
- Creates penalties for disclosing "individually identifiable health information."
- As extreme as up to 10 years imprisonment and $250,000 fine

HITECH

- "Health Information Technology for Economic and Clinical Health"
- 42 U.S.C. § 300jj et seq.
- Required disclosure of breach by covered entity
- Civil penalties 42 U.S.C. § 17939(c)-(d)
- Criminal prosecution 42 U.S.C. § 17940

Compliance

- Business Associate Agreement
- Notice of Breach
- Mitigation and Remediation Response
- Report to Law Enforcement
- Use compliant cloud services

What is Encryption?

Basically encoding data

Data gets scrambled

- Example: Happy becomes Paphy

Requires key to decode and unscramble

Very Common

Encryption

Pros

- Protects Data
- Simple to implement
- Common

Cons

- Slows down data transfer
- Only as good as key
- Lost key = lost data (usually)

eFiling

Free service through efile.txcourts.gov	• Free! • eFiled documents available for 15 days
Paid services (numerous brands)	• Support • Additional Services (searchable PDF, eFax, better proof of service) • Documents may be available longer

eFiling Service Providers

eFile Texas

File Time Texas

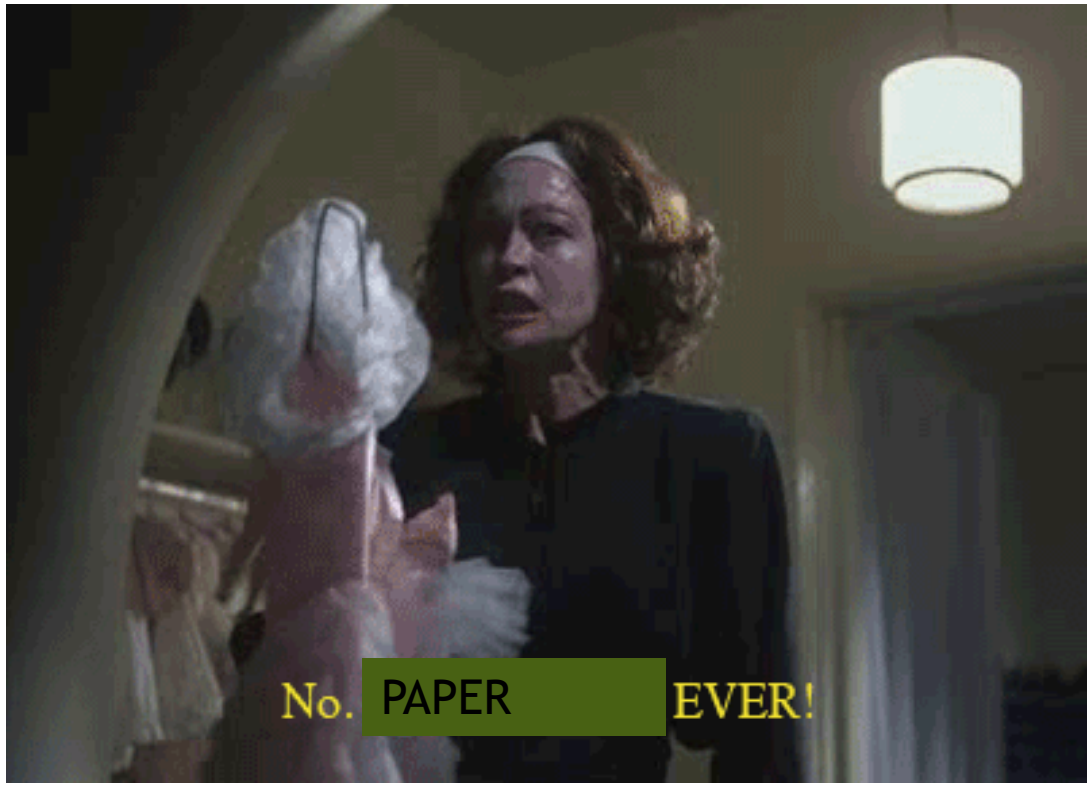
One Legal

Green Filing Texas

ProDoc

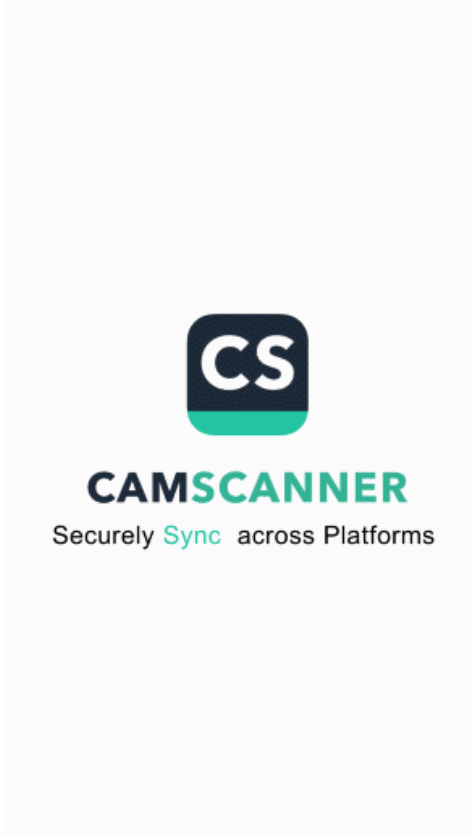
Warning:

This is me with paper in my office.



MY BEST CO-WORKER

2nd Place BEST CO-WORKER



Communicating with your client, the court, opposing counsel, and others

- Email
- Text Messaging
- Instant Messaging – Facebook or AIM
- Document Cloud – Adobe Document
- Document Management Software ie Cloud Storage – Dropbox & Box
- Client Management Software ie Client Relationship Management

Email

Pros

- Very Easy
- Free in most cases
- Quick
- Anytime
- Attachments
- Copied to others and files
- Proof of Receipt
- Prepared in Advance
- Encrypted

Cons

- Must have an email
- Must have access to internet
- Must know the email address
- People change their emails
- Employees send to friends
- Emails could get lost in the numbers
- Viruses
- Some companies restrict attachments
- Email scams

Text Messaging

Pros

- Send anytime
- Mobile Phone can be off
- Save time
- Does not interrupt someone
- Informal messages
- Easy to keep in touch

Cons

- Only short messages
- Tiny Mobile Phone Keybpads
- Basic Typing Skills needed
- Text speak destroys grammar
- DO NOT FIRE PEOPLE

Instant Messaging

Pros

- Real Time
- Keeps you connected
- Customer Support Contact instead of a phone support line

Cons

- No time to reflect on your words
- Advertisements
- Anyone can usually send you one

Document Cloud

Pros

- Minimal Hassle
- Integrates with other software
- Save files into one cloud
- Can Sign documents on phone
- No special software required
- Edit and share PDF files
- Track
- Organization of many files into one

Cons

- Products on multiple computers
- Costs per user
- Installation can be complex
- Can be slow

Document Management Software

Pros

- Accessed anywhere by internet
- Scalable
- Pay only what you need
- Less IT staff
- Can move offices quickly

Cons

- Slow internet connections
- Data security
- Requires Encrypting
- Limitation of Bandwidth
- Ongoing Costs

Client Management Software

Pros

- Everything in one place
- Scalable Solutions
- Data Mining
- Remote access
- Speed up conversion
- Lowers daily costs

Cons

- Eliminates human element
- Security Issues
- Learning Curve
- Spotty technical support
- Lost data if database is lost
- Sensitive Data into third party