The following chapter is an excerpt from **Locked Down: Practical Information Security for Lawyers** (ABA, 2016) by Sharon D. Nelson, David G. Ries and John W. Simek. The book may be purchased at http://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=238368703

Lawyers' Duty to Safeguard Information

Confidential data in computers and information systems, including those used by attorneys and law firms, faces greater security threats today than ever before. And they continue to grow! These threats are substantial and real. As discussed in our previous chapter on data breach nightmares, they have taken a variety of forms, ranging from phishing scams and social engineering attacks (e.g., using e-mail to trick attorneys to visit a malicious web site or to be lured into fraudulent collection schemes for foreign "clients") to sophisticated technical exploits that result in long term intrusions into a law firm's network to steal information. They also include inside threats - malicious, untrained, inattentive, and even bored personnel – and lost and stolen laptops and mobile devices.

Attorneys have ethical, common law and statutory obligations to protect information relating to clients. Many attorneys also have contractual obligations to protect data. Beyond these requirements, protection of confidential information is sound business and professional practice. It is critical for attorneys to understand and address these obligations and to exercise constant vigilance to protect client data and other confidential information.

Ethical Duties Generally

An attorney's use of technology presents special ethics challenges, particularly in the areas of competence and confidentiality. The duty of competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to appropriately and securely use it. This duty also requires attorneys who lack the necessary technical competence to either learn what is necessary or consult with qualified people who have the requisite expertise. The duty of confidentiality (ABA Model Rule 1.6) is one of an attorney's most important ethical responsibilities. Together, these rules (included in Appendix D) require attorneys using technology to take competent and reasonable measures to safeguard information relating to clients. It is a continuing obligation as technology, threats and available security measures evolve. This duty extends to all use of technology, including computers, portable devices, networks, technology outsourcing and cloud computing. Effective information security is an ongoing process that requires constant vigilance.

Model Rule 1.1 covers the general duty of competence. It provides that "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology.

Model Rule 1.6 generally defines the duty of confidentiality. It begins as follows:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

Rule 1.6 broadly requires protection of "information relating to the representation of a client"; it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The Ethics 2000 revisions to the model rules (over 10 years ago) added Comment 16 to Rule 1.6. This comment requires reasonable precautions to safeguard and preserve confidential information.

> **Acting Competently to Preserve Confidentiality**
>
> [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

The ABA Commission on Ethics 20/20 conducted a review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. One of its core areas of focus was technology and confidentiality. Its Revised Draft Resolutions in this area were adopted by the ABA at its Annual Meeting in August of 2012.[1]

The amendments include addition of the following highlighted language to the Comment to Model Rule 1.1 Competence:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology…

The amendments also added the following new subsection (highlighted) to Model Rule 1.6 Confidentiality of Information:

> (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

This requirement covers two areas – inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, erroneously producing privileged documents or data, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The amendments also include the following changes to Comment [18] to this rule:

> **Acting Competently to Preserve Confidentiality**
>
> [18] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or

[1] See, www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.

> unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Significantly, these revisions are clarifications rather than substantive changes. They add additional detail that is consistent with the then existing rules and comments, ethics opinions, and generally accepted information security principles.[2]

Model Rule 1.4 also applies to attorneys' use of technology. It requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished." It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." As stated in ABA Formal Ethics Opinion 95-398, "Access of Nonlawyers to a Lawyer's Database" (October 27, 1995), it may require notice to a client of compromise of confidential information relating to the client if the release of information "could reasonably be viewed as a significant factor in the representation."

The comment references Model Rule 5.1 (Responsibilities of Partners, Managers, and Supervisory Lawyers) and Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants), which are also important in attorneys' use of technology. Partners and supervising attorneys (including junior attorneys supervising staff or service providers) are required to take reasonable actions to ensure that those under their supervision comply with these requirements.

Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) was amended to expand its scope. "Assistants" was expanded to "Assistance," extending its coverage to all levels of staff and outsourced services ranging from copying services to outsourced legal services. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to

---

[2] ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised* (2012): "The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent." (Model Rule 1.1) "This duty is already described in several existing Comments, but the Commission concluded that, in light of the pervasive use of technology to store and transmit confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6."

insure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's duty of confidentiality.

Attorneys must also take reasonable precautions to protect confidential information to which third parties, like information systems consultants and litigation support service providers, are given access. ABA Formal Ethics Opinion 95-398, provides guidance in this area and concludes, "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information."

In August 2008, the ABA issued an ethics opinion that comprehensively addresses outsourcing by attorneys of both legal services and nonlegal support services. ABA Formal Ethics Opinion 08-451, "Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services" (August 2008). It includes requirements for protecting confidentiality.

A 2011 Pennsylvania opinion (included in Appendix E) analyzes ethics requirements for attorneys' use of cloud computing, a form of outsourcing. Formal Opinion 2011-200, "Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property." It concludes:

> An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

These requirements are further discussed in our chapters on outsourcing and cloud computing.

A number of state ethics opinions have addressed professional responsibility issues related to attorneys' use of various technologies. Several examples are discussed in this chapter. It is important for attorneys to consult the rules, comments and ethics opinions in the relevant jurisdiction(s).

An early ethics opinion on this subject, State Bar of Arizona, Opinion No. 05-04, "Formal Opinion of the Committee on the Rules of Professional Conduct" (July 2005), provides a well-reasoned explanation of these duties for electronic files and communications. It notes that "an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." The opinion also calls for "competent and reasonable measures to assure that the client's electronic information is not lost or destroyed." It further notes that "an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence."

An April 2006 New Jersey ethics opinion takes a consistent approach in reviewing obligations in lawyers' use of electronic storage and access of client files. New Jersey Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage and Access of Client Files" (April 2006). It observes:

> The obligation to preserve client confidences extends beyond merely prohibiting an attorney from himself making disclosure of confidential information without client consent (except under

> such circumstances described in RPC 1.6). It also requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure. . . .
>
> The critical requirement under RPC 1.6, therefore, is that the attorney "exercise reasonable care" against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access. "Reasonable care," however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room or that someone will not illegally intercept his mail or steal a fax.

A later Arizona opinion contains a similar analysis, with emphasis on requirements of awareness of limitations of lawyers' knowledge of technology and periodic review of security measures. State Bar of Arizona, Opinion No. 09-04, "Confidentiality; Maintaining Client Files; Electronic Storage; Internet" (Formal Opinion of the Committee on the Rules of Professional Conduct) (December 2009). It explains,

> Lawyers providing an online file storage and retrieval system for client access of documents must take **reasonable precautions** to protect the security and confidentiality of client documents and information. Lawyers should be **aware of limitations in their competence** regarding online security measures and take appropriate actions to ensure that a competent review of the proposed security measures is conducted. As technology advances over time, a **periodic review** of the reasonability of security precautions may be necessary.

A recent California ethics opinion addresses the use of a laptop by an attorney, where the laptop may be monitored by the law firm, and use of the laptop in public and home wireless networks. The opinion concludes that such use may be proper under the ethics rules if an adequate evaluation is made and appropriate precautions are taken. State Bar of California, Formal Opinion No. 2010-179 (included in Appendix F).

The Digest to this opinion states:

> Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

The opinion contains a detailed analysis of the ethics requirements for attorneys' use of technology and their application to the technology covered in the opinion, including a detailed discussion of factors an attorney should consider before using a specific technology. Significantly, it includes the requirement of an evaluation **before** an attorney uses a particular technology.

Attorneys need to stay up to date as technology changes and new threats are identified. For example, following news reports that confidential information had been found on digital copiers that were ready for resale,[3] the Florida Bar issued Professional Ethics of the Florida Bar Opinion 10-2 (September, 2010) that addresses this risk. Its conclusion states:

> In conclusion, when a lawyer chooses to use Devices that contain Storage Media, the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

New York Opinion 1019, "Remote Access to Firm's Electronic Files" (August 2014), cautions attorneys to analyze necessary precautions in the context of current risks:

> Cybersecurity issues have continued to be a major concern for lawyers, as cybercriminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cybercrooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system.

It leaves it up to attorneys and law firms to determine the specific precautions that are necessary:

> Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information.

The opinion requires attorneys to either make a determination that the selected precautions provide reasonable protection, in light of the risks, or to obtain informed consent from clients after explaining the risks.

---

[3] E.g., Armen Keteyian, "Digital Copiers Loaded with Secrets," *CBS Evening News* (April 19, 2010). www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets.

There are now multiple ethics opinions on attorneys' use of cloud computing services like online file storage and software as a service (SaaS).[4] For example, New York Bar Association Committee on Professional Ethics Opinion 842 "Using an outside online storage provider to store client confidential information" (September, 2010), consistent with the general requirements of the ethics opinions above, concludes:

> A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.

Additional examples of opinions covering cloud services are Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200, "Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (November, 2011) and North Carolina State Bar 2011 Formal Ethics Opinion 6, "Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (January, 2012).

The key professional responsibility requirements from these various opinions on attorneys' use of technology are **competent and reasonable measures to safeguard client data**, including an understanding of limitations in attorneys' competence, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available security evolve.

Ethical Duties: Electronic Communications

E-mail and electronic communications have become everyday communications forms for attorneys and other professionals. They are fast, convenient, and inexpensive, but also present serious risks. It is important for attorneys to understand and address these risks.

In addition to adding the requirement of reasonable safeguards to protect confidentiality, the Ethics 2000 revisions to the Model Rules, over 10 years ago, also added Comment 17 [now 19] to Rule 1.6. This comment requires reasonable precautions to safeguard and preserve confidential information during electronic transmission. This Comment, as amended in accordance with the Ethics 20/20 recommendations (highlighted), provides:

---

[4] The ABA Legal Technology Resource Center has published a summary with links, "Cloud Ethics Opinions around the U.S.," available at www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

This Comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as providing that attorneys never need to use "special security measures" like encryption.[5] While it does state that "special security measures" are not generally required, it contains qualifications and notes that "special circumstances" may warrant "special precautions." It includes the important qualification - "if the method of communication affords a reasonable expectation of privacy." There are, however, questions about whether unencrypted Internet e-mail affords a reasonable expectation of privacy.

[5] Encryption is a process that translates a message into a protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. E-mail encryption has become easier to use over time. Transport layer security (TLS) encryption is available to automatically encrypt e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to automatically encrypt all e-mails between them. A virtual private network is an arrangement in which all communications between two networks or between a computer and a network are automatically protected with encryption. See, David G. Ries and John W. Simek, "Encryption Made Simple for Lawyers," *GPSolo Magazine* (November/December 2012).

Respected security professionals for years have compared e-mail to postcards or postcards written in pencil.[6] A June 2014 post by Google on the *Google Official Blog*[7] and a July 2014 *New York Times* article[8] use the same analogy – comparing unencrypted e-mails to postcards. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada[9] and Massachusetts[10] (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like these, it will become more difficult for attorneys to demonstrate that confidential client data needs lesser protection.

Comment 19 also lists as a consideration "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act[11] and similar state laws make unauthorized interception of electronic communications a crime. Some observers have expressed the view that this should be determinative and attorneys are not required to use encryption. The better view is to treat legal protection as only one of the factors to be considered. As discussed above, some of the newer ethics opinions conclude that encryption may be a reasonable measure that should be used, particularly for highly sensitive information.

An ABA ethics opinion in 1999 and several state ethics opinions have concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail.[12] However, these

---

[6] E.g., B. Schneier, *E-Mail Security - How to Keep Your Electronic Messages Private,* (John Wiley & Sons, Inc. 1995) p. 3; B. Schneier, *Secrets & Lies: Digital Security in a Networked Work*, (John Wiley & Sons, Inc. 2000) p. 200 ("The common metaphor for Internet e-mail is postcards: Anyone – letter carriers, mail sorters, nosy delivery truck drivers - who can touch the postcard can read what's on the back."); and Larry Rogers, *Email – A Postcard Written in Pencil*, Special Report, (Software Engineering Institute, Carnegie Mellon University 2001).

[7] "Transparency Report: Protecting Emails as They Travel Across the Web," *Google Official Blog* (June 3, 2014) ("…we send important messages in sealed envelopes, rather than on postcards. …Email works in a similar way. Emails that are encrypted as they're routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards.")
http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html.

[8] Molly Wood, "Easier Ways to Protect Email From Unwanted Prying Eyes," *New York Times* (July 16, 2014) ("Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit. The government can probably read your email, as can hackers and your employer.")
www.nytimes.com/2014/07/17/technology/personaltech/ways-to-protect-your-email-after-you-send-it.html?_r=0.

[9] Nev. Rev. Stat. 603A.010, *et seq.*

[10] Mass. Gen. Laws Ch. 93H, regulations at 201 CMR 17.00.

[11] 18 U.S.C. §§ 2510 et seq.

[12] E.g., ABA Formal Opinion No. 99-413, *Protecting the Confidentiality of Unencrypted E-Mail* (March 10, 1999) ("based upon current technology and law as we are informed of it …a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a)…" "…this opinion does not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication,

opinions should be carefully reviewed because, like Comment 19, they contain qualifications that limit their general conclusions. In addition, more recent ethics opinions, discussed below, are increasingly recognizing that encryption may be a required safeguard, at least in some circumstances.

For example, New York Bar Association Committee on Professional Ethics Opinion 709 "Use of Internet to advertise and to conduct law practice focusing on trademarks; use of Internet e-mail; use of trade names" (September, 1998) concludes:

> We therefore conclude that lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality … to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use e-mail for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.
>
> A lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost. It is also sensible for lawyers to discuss with clients the risks inherent in the use of Internet e-mail, and lawyers should abide by the clients' wishes as to its use.

Consistent with the questions about the security of e-mail, some ethics opinions express a stronger view that encryption may be required. For example, New Jersey Opinion 701 (April, 2006), discussed above, notes at the end: "where a document is transmitted to [the attorney]… by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access."[13] This was over 9 years ago.

California Formal Opinion No. 2010-179, also discussed above, notes that "encrypting email may be a reasonable step for an attorney in an effort to ensure the confidentiality of such communications

---

the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.") and District of Columbia Bar Opinion 281, "Transmission of Confidential Information by Electronic Mail," (February, 1998), ("In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.").

[13] File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. It is generally easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that are easy to break or "crack."

remain so when circumstances call for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous."

An Iowa opinion on cloud computing suggests the following as one of a series of questions that attorneys should ask when determining appropriate protection: "Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?" Iowa Ethics Opinion 11-01.

A Pennsylvania ethics opinion on cloud computing concludes that "attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality." It discusses encryption as an additional precaution that may be required when using services like web mail. Pennsylvania Formal Opinion 2011-200.

Texas Ethics Opinion 648 (2015) takes the same approach:

> 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.

The opinion includes examples of circumstances where encryption may be required.

Summarizing these more recent opinions, a July, 2015 ABA article notes:[14]

> The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required.

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients (preferably in an engagement letter or other writing) about the nature of communications that will be (and will not be) sent electronically and whether or not encryption and other security measures will be utilized.

It has now reached the point (or at least is reaching it) where all attorneys should have encryption available for use in appropriate circumstances.

Common Law Duties

In addition to the duties arising from applicable rules of professional conduct, there are parallel common law duties to protect confidentiality. These duties are defined by case law in the various states. The Restatement (Third) of the Law Governing Lawyers (2000) summarizes this area of the law. See Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client's confidences, and Chapter 5, "Confidential Client Information." Breach of these common law duties may result in malpractice liability.

There are also instances when lawyers have contractual duties to protect client data. This is particularly the case for clients in regulated industries, such as health care and financial services, that have

---

[14] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," *Eye on Ethics, Your ABA* (July 2015) www.americanbar.org/publications/youraba/2015/july-2015/encryption-conniption.html.

regulatory requirements to protect privacy and security. Clients are recognizing that law firms may be the weak links in protecting their confidential information and are increasingly requiring specified safeguards, providing questionnaires about a law firm's security, and even requiring security audits.[15]

Attorneys and law firms who accept credit cards are "merchants" that are required to comply with the Payment Security Industry Data Security Standard (PCI). It is generally required under the merchant processing agreement with a bank or processor.

Statutes and Regulations

In addition to the ethical and common law duties to protect client information, various state and federal statutes and regulations require protection of defined categories of personal information. Some of them are likely to apply to lawyers who possess any covered personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses.

At least 12 states now have general information security laws that require reasonable measures to protect defined categories of personal information (including Arkansas, California, Connecticut, Illinois, Maryland, Massachusetts, Nevada, New Jersey, Oregon, Rhode Island, Texas, and Utah). While the scope of coverage, the specificity of the requirements, and the definitions vary among these laws, "personal information" is usually defined to include general or specific facts about an identifiable individual. The exceptions tend to be information that is presumed public and does not have to be protected (e.g., a business address).

The most comprehensive law of this type to date is a Massachusetts law,[16] which applies to "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." Covered "personal information" includes Social Security numbers, driver's license numbers, state-issued identification card numbers, financial account numbers and credit card numbers. With its broad coverage of "persons," this law is likely to be applied to persons nationwide, including attorneys and law firms, when they have sufficient contacts with Massachusetts to satisfy personal jurisdiction requirements. It requires covered persons to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."

The implementing regulation, 201 CMR 17 (included in Appendix B), became effective on March 1, 2010. It requires covered persons to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards." The regulation contains detailed requirements for the information security

---

[15] Kenneth N. Rashbaum, Jason M. Tenenbaum and Liberty McAteer, "Cybersecurity: Business Imperative for Law Firms," New York Law Journal (December 10, 2014) www.newyorklawjournal.com/id=1202678493487/Cybersecurity-Business-Imperative-for-Law-Firms?slreturn=20141127155939 and Sharon D. Nelson & John W. Simek, "Clients Demand Law Firm Cyber Audits," *Law Practice* (November/December 2013) www.americanbar.org/publications/law_practice_magazine/2013/november-december/hot-buttons.html.

[16] Mass. Gen. Laws Ch. 93H.

program, including a risk assessment, assigning responsibility for security, training requirements and requiring security for third parties who are given access to protected information. It also includes detailed computer system security requirements. The requirements include the following, with subparts requiring additional details:

- Secure user authentication protocols.
- Secure access measures.
- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- Reasonable monitoring of systems for unauthorized use of or access to personal information.
- Encryption of all personal information stored on laptops or other portable devices.
- For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches (fixes issued by the manufacturer), reasonably designed to maintain the integrity of the personal information.
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Lawyers and law firms should understand the requirements of the Massachusetts law because they may directly apply, they are based on generally accepted security principles, and some observers believe that they will become a model for legal requirements for comprehensive protection of personal information.

Nevada also has laws that require “reasonable security measures” and encryption (NRS 603A.210 and NRS 597.970), although they are much less detailed than the Massachusetts law. In addition, encryption is already required for federal agencies that have information about individuals on laptops and portable media. As encryption becomes a security standard, it is likely to become the standard of what is reasonable for lawyers.

The legal obligations don’t stop, however, at requiring these kinds of measures to protect the confidentiality of information. Forty-seven states and the District of Columbia and the Virgin Islands have laws that require notification concerning data breaches (all but Mississippi, New Mexico and South Dakota). While there are differences in their scope and requirements, they generally require entities that own, license or possess defined categories of personally identifiable information about consumers to notify affected consumers if there is a breach. Like the reasonable security laws, many of these laws apply to covered information “about” residents of the state. Some require notice to a state agency in addition to notice to consumers. Most of these laws have encryption safe harbors, which provide that notice is not required if the data is encrypted and the decryption key has not been compromised.

To add to the web of issues involved, at least 19 states also now have laws that require secure disposal of paper and electronic records that contain defined personal information. The Federal Trade

Commission's Disposal Rule[17] has similar requirements for consumer credit reports and information derived from them.

At the federal level, an attorney who receives protected personally identifiable health information (PHI) from a covered entity under the Health Insurance Portability & Accountability Act (HIPAA) will generally be a "business associate" and be required to comply with the HIPAA security requirements. The 2009 Healthcare Information Technology and Clinical Health (HITECH) Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement.

Standards for Competent and Reasonable Measures

The core challenge for lawyers and law firms in establishing information security programs is deciding what security measures are necessary and then implementing and maintaining them. Determining what constitutes "competent and reasonable measures" can be difficult. If attorneys are governed by legal requirements like HIPAA or the new Massachusetts law, they must comply with these requirements. Consensus government and industry standards are now commonly used by law firms, as well as other businesses and enterprises, in determining what constitutes reasonable security. Legal standards that apply in other areas, like health care and financial services, can also be helpful in providing a framework for security, even where they do not legally apply.

Consensus government and industry standards are discussed in the next chapter. Commonly used examples are those published by the National Institute for Standards and Technology (NIST), part of the U.S. Department of Commerce, like *its Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (February 2014) and its *Small Business Information Security: the Fundamentals, Draft NISTIR 7261, Rev. 1* (December 2014). Standards like those published by the International Organization for Standardization (ISO) (available at www.iso.org) are also being commonly used, particularly by larger firms. They include ISO/IEC 27002:2013, "Information Technology—Code of Practice for Information Security Management," ISO/IEC 27001:2013, "Information Technology—Security Techniques—Information Security Management System— Requirements," and others.

The FTC's Safeguards Rule under the Gramm-Leach-Bliley Act (included in Appendix H) also provides a helpful basic framework that lawyers can use to assist in complying with their obligations to safeguard client data, even when it is not a legal requirement. The requirements in the rule, "Standards for Safeguarding Customer Information," 16 CFR, Part 314, are general and cover fewer than two pages in the Federal Register.

Legal groups, including the American Bar Association, state bars, and the International Legal Technology Association (ILTA) LegalSEC initiative have been working to tailor these kinds of standards for attorneys and law firms. Details are discussed in the information security overview chapter.

In addition to considering frameworks and standards like these, attorneys should also consider generally accepted security practices. For example, after the high-profile theft of a Department of Veterans Affairs laptop and portable drive containing personal information on more than 28 million veterans in 2006, the Office of Management and Budget (OMB) issued new security guidelines for federal agencies. They

[17] 16 C.F.R. Part 682.

require encryption of laptops and mobile devices. (The OMB memorandum dated June 23, 2006, is included in Appendix K.) Both before this incident and increasingly since it, encryption of laptops and mobile devices containing confidential has become a standard security practice.

Despite this standard practice, there have been a number of reported thefts and losses of unencrypted laptops and portable drives from law firms. There most likely have been many more that have not been disclosed. The *Verizon 2014 Data Breach Investigation Report*, which covers 2013, explains the risk of lost and stolen devices and a solution to it—encryption—this way: [18]

> *PHYSICAL THEFT AND LOSS—RECOMMENDED CONTROLS*
>
> The primary root cause of incidents in this pattern is carelessness of one degree or another. Accidents happen. People lose stuff. People steal stuff. And that's never going to change. But there are a few things you can do to mitigate that risk.
>
> **Encrypt devices**
>
> Considering the high frequency of lost assets, **encryption is as close to a no-brainer solution as it gets for this incident pattern**. Sure, the asset is still missing, but at least it will save a lot of worry, embarrassment, and potential lawsuits by simply being able to say the information within it was protected.
> (Emphasis added.)

It's not just Verizon; this view is widely held by information security professionals and government agencies.[19] This raises the question: Are attorneys who are not using encryption for laptops and mobile devices taking competent and reasonable measures to protect them?

Conclusion

Confidential data in attorneys' computers and information systems today faces substantial, real, and growing security risks. It is critical for attorneys to understand and address these risks to comply with their ethical, common law, and regulatory obligations to safeguard confidential data. Fortunately, these duties do not require attorneys to become computer scientists or security specialists (the last thing that most attorneys want to do). They do require attorneys to be aware of the risks and security requirements and to ensure that security is adequately addressed, including the involvement of qualified professionals where necessary. Constant security awareness by attorneys and staff is key. Finally, information security is an ongoing duty as technology, risks and available security measures change over time.

Selected Ethics Opinions: Technology, the Internet and Cloud Computing

ABA Formal Ethics Opinion 11-459, "Duty to Protect the Confidentiality of E-Mail Communications with One's Client," (August 2011)

---

[18] www.verizonenterprise.com/DBIR/2014.

[19] E.g., US-CERT, the National Institute of Science and Technology (NIST), the Federal Communications Commission, and the Department of Health and Human Services have all recommended or required encryption on mobile devices to protect confidential information.

ABA Formal Ethics Opinion 08-451, “Lawyer’s Obligations When Out- sourcing Legal and Nonlegal Support Services” (August 2008)

ABA Formal Ethics Opinion 99-413, “Protecting the Confidentiality of Unencrypted E-Mail” (March 1999)

ABA Formal Ethics Opinion 95-398, “Access of Nonlawyers to a Lawyer’s Data Base” (October 1995)

Alabama Ethics Opinion 2010-02, “Retention, Storage, Ownership, Production and Destruction of Client Files” (includes cloud computing)

State Bar of Arizona, Opinion No. 05-04, “Electronic Storage; Confidentiality” (July 2005)

State Bar of Arizona, Opinion No. 09-04, “Confidentiality; Maintaining Client Files; Electronic Storage; Internet” (December 2009)

State Bar of California, Formal Opinion No. 2010-179, “Use Of Technology to Transmit or Store Confidential Client Information, Including Public and Home Wireless Networks,” (a copy is included in Appendix F)

Professional Ethics of the Florida Bar, Opinion 06-1, “Electronic File Storage” (April 2006)

Illinois State Bar Association, Opinion 10-01, “Law Firm Computer Network Managed by Offsite Third-Party Vendor” (July 2009)

Maine Professional Ethics Commission, Opinion #194, “Client Confidences: Confidential Firm Data Held Electronically and Handled by Technicians for Third-Party Vendors” (June 2008)

Massachusetts Bar Opinion 2005-04, “Third-Party Software Vendor Access to Confidential Client Information Stored on the Firm’s Computer System for the Purpose of Allowing the Vendor to Support and Maintain a Computer Software Application Utilized by the Law Firm” (March 2005)

State Bar of Nevada, Formal Opinion No. 33, “Use of Outside Party to Store Electronic Client Information” (February 2006)

New Jersey Advisory Committee on Professional Ethics, Opinion 701, “Electronic Storage and Access of Client Files” (April 2006)

New York State Bar Association, Committee on Professional Ethics, Opinion 1020, “Confidentiality: Use of Cloud Storage for Purposes of a Transaction” (September 2014)

New York State Bar Association, Committee on Professional Ethics, Opinion 1019, “Remote Access to Firm’s Electronic Files” (August 2014)

New York State Bar Association, Committee on Professional Ethics, Opinion 842, “Using an Outside Online Storage Provider to Store Client Confidential Information” (September 2010)

New York State Bar Association, Committee on Professional Ethics, Opinion 820, “Use of E-Mail Service Provider That Scans E-Mails for Advertising Purposes” (February 2008)

North Carolina Proposed 2011 Formal Ethics Opinion 7, “Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property” (October 2011)

Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200, “Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property” (November 2011) (a copy is included in Appendix E)

State Bar of Texas, Professional Ethics Committee, Opinion No. 648 (communicating confidential information by email) (April 2015)

Virginia Legal Ethics Opinion 1818, “Whether the Client’s File May Contain Only Electronic Documents with No Paper Retention?” (September 2005)