Law Firm Cybersecurity Requirements You Never Dreamed Of: Emerging Threats, Ethical Obligations to Clients, and Survival Tactics

CLE MATERIALS

ABA Annual Meeting Showcase
Sponsored by the ABA Cybersecurity Legal Task Force
Friday, August 9, 2019, 2:00-3:30 pm PT

Table of Contents


▪ ABA Formal Opinions, ABA Standing Committee on Ethics and Professional Responsibility
  o ABA Formal Opinion 483, “Lawyers’ Obligations After an Electronic Data Breach or Cyberattack” (October 17, 2018)
  o ABA Formal Opinion 482, “Ethical Obligations Related to Disasters” (September 19, 2018)
  o ABA Formal Opinion 477R*, “Securing Communication of Protected Client Information” (May 11, 2017 Revised May 19, 2017)


Additional Resources

▪ For cybersecurity/data protection information, see the website of the ABA Cybersecurity Legal Task Force (co-chaired by Ruth Hill Bro and Thomas J. Smedinghoff), which focuses and coordinates the ABA’s cybersecurity legal and policy analyses/assessments and identifies, compiles, and creates cybersecurity resources from a cross-disciplinary perspective, at www.ambar.org/cyber.
  o Includes link to the Task Force’s “Vendor Contracting Project: Cybersecurity Checklist” (FREE).
Includes link to a list of cybersecurity resources for solo/small law firms and businesses.

- **For the ABA Cybersecurity Legal Task Force’s cybersecurity webinar series**, see “Cybersecurity Wake-Up Call: The Business You Save May Be Your Own” (a 5-part webinar series based on the Task Force’s 2018 *ABA Cybersecurity Handbook*), at ambar.org/cyberwakeup (recorded programs, including ethics credit).

- **For Digital Dangers (a yearlong exploration of cybersecurity and the law)**, jointly produced by the *ABA Journal* and the ABA Cybersecurity Legal Task Force (2018), see articles at abajournal.com/magazine/cyber (FREE).
Chapter 6

Lawyers’ Obligations to Provide Data Security Arising from Ethics Rules and Other Law

Peter Geraghty and Lucian T. Pera

Like all their professional activities, the obligation of lawyers to secure their clients’ sensitive information is defined and governed by ethics rules, common law, and statutes that traditionally cover the activities of lawyers.

I. ABA Formal Opinion 477R

Immediately before the publication of this edition of the Handbook, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Ethics Opinion 477R (revised May 22, 2017), which will likely become its seminal guidance on a lawyer’s ethical obligation to maintain the security of client confidential information in today’s digital information environment. This opinion provides a broad framework for understanding the ethical obligation at the heart of this chapter, and directly informs the more detailed discussion that follows. Any reader of this chapter should also review in detail new ABA Formal Opinion 477R.

This new opinion first reviews the ABA's most prominent earlier opinion in this area, ABA Formal Opinion 99-413 (March 10, 1999), which generally blessed lawyer use of unencrypted Internet e-mail for client confidential information. The new opinion then reviews the 2012 “technology amendments” to the ABA Model Rules of Professional Conduct, discussed in more detail below. These amendments, now adopted in 27 U.S. jurisdictions, generally confirm, clarify, and remind lawyers of their ethical obligations concerning the use of information technology and the protection of client confidentiality in a rapidly changing environment. These amendments confirm that, in the central tenet of amended Rule 1.6(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” (emphasis added).

Nothing in this new opinion makes obsolete earlier guidance from the ABA and other authorities. Formal Opinion 477R does, however, reject an overly broad interpretation of earlier ABA Formal Opinion 99-413, which some read to mean that a lawyer was ethically permitted to use unencrypted e-mail for client confidential communications in every circumstance.

Quoting the first edition of this book, Opinion 477R states that in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.3

---

This new opinion then reviews in some detail some of the factors that should guide lawyers in making a “reasonable efforts” analysis, including factors set out in revised Comment [18] to Rule 1.6, discussed below. Applying these factors to lawyer use of unencrypted e-mail to communicate client confidential information, the committee concludes that, given today’s technology and threat environment, while unencrypted e-mail may well be appropriate for routine communications including information of “normal or low sensitivity,” transmitting “highly sensitive information” might require more secure communications technology or even avoiding the use of electronic communications altogether.

The opinion then identifies and explores a series of pragmatic considerations that a lawyer may consider in seeking to use “reasonable efforts” to protect client confidential information:

1. Understand the Nature of the Threat.
2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.
5. Label Client Confidential Information.
7. Conduct Due Diligence on Vendors Providing Communication Technology.4

Finally, Opinion 477R emphasizes the need and duty of a lawyer to communicate with the client about the sensitivity of information concerning the representation and the appropriate means and methods of protecting confidentiality. In many ways, this new opinion distills the ethics guidance of the last 20 years and updates it in light of the current technology environment. Aligned with this opinion, this chapter reviews existing guidance

and demonstrates how the broader principles restated and reformulated in Opinion 477R apply to particular circumstances faced by lawyers in their practice.

II. Lawyer Ethics Rules

A. Confidentiality

Lawyers and law firms must adopt safeguards to protect their clients’ information because they have an ethical duty to keep that information confidential. ABA Model Rule 1.6(a) states that, with limited exceptions, “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” This obligation to maintain confidentiality of all information concerning a client’s representation, no matter the source, is paramount. The obligation is no less applicable to electronically stored information than to information contained in paper documents or not reduced to any written or stored form.

So what does this mean? What steps must a lawyer take to protect the client’s information? The last major review and revision of the ABA Model Rules of Professional Conduct was led by the ABA Ethics 20/20 Commission.5 In the area of issues raised by new technology, the signature change made to the Model Rules by the Ethics 20/20 Commission was the addition of a new section to the core rule on client confidentiality. This new Rule 1.6(c) codified the existing understanding of a lawyer’s affirmative obligation to protect confidential information: “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.” While this revision merely confirms prior law under the ethics rules of every

---

5. Created by then ABA President Carolyn B. Lamm in 2009, the Ethics 20/20 Commission performed a thorough 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. Further information about the commission is available at ABA Commission on Ethics 20/20, https://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.
American jurisdiction, versions of these revisions have been adopted by at least 27 U.S. jurisdictions as of this writing.

Revised Comments [17] and [18] to Rule 1.6 also now include more detailed guidance—guidance largely consistent with existing rules in virtually every jurisdiction—concerning how to measure the reasonableness of a lawyer’s efforts to protect against inadvertent disclosure or unauthorized access. This language forms the core set of principles used throughout virtually all ethics opinions in American jurisdictions that address confidentiality concerns in the cybersecurity context. Comment [17] sets out how reasonableness under Rule 1.6(c) should be determined:

Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, 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 forgo security measures that would otherwise be required by this Rule.

The comment goes on to note that “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,” but that any such obligations are “beyond the scope of these Rules.”

Comment [17] concludes the Model Rules’ framing of a lawyer’s obligations to maintain the security of client confidential information, including its limits:

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.

In effect, this comment envisages a balancing test: the more sensitive the data being transmitted and the lower the legal or technological protection afforded by the method of communication, the more likely it is that special precautions may be reasonably necessary to protect client confidences.

From 2013 through 2015, the ABA, through its House of Delegates, approved a series of resolutions proposed by the ABA’s Cybersecurity Task Force that highlighted the threat of cyber attacks on lawyers and law firms. In Revised Report 109 (2014), the Task Force observed:

The threat of cyber attacks against law firms is growing. Lawyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices. There are many reasons for hackers to target the information being held by law firms. They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data and litigation-related theories and records collected through e-discovery.

That threat continues to grow.

A number of state bar ethics opinions have addressed a lawyer’s obligations to protect client confidential information in this age of electronic communications. The focus of these opinions ranges from suggested security safeguards to an examination of new technologies and the need for lawyers to have a basic understanding of the risks and benefits associated with them.
1. State Bar Opinions: Suggested Safeguards

Some state bar associations have issued ethics opinions that suggest specific measures that a law firm should take to protect their clients’ electronically stored information. For example, Arizona State Bar Opinion 09-04 (2009) provides some examples of what lawyers should be doing to secure their clients’ electronically stored information: “In satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc.”

The client file system that was the subject of this Arizona opinion protected the files by using a method of encryption and also applied several layers of password protection. Additionally, the system used unique and randomly generated folder names and passwords, and converted each document to PDF format that required yet another unique alpha-numeric password to review its contents. Based on these safeguards, this Arizona opinion concluded that the file system met the requirements set forth by Rule 1.6.6

2. State Bar Opinions: Technology as Moving Target

Other state bar opinions have recognized, as did ABA Opinion 477R, that the swiftly changing nature of technology makes it very difficult to identify specific security measures that lawyers should take that will invariably ensure that confidential client information will be protected.7 Accordingly, their focus is on the scope of the lawyer’s obligations to take reasonable precautions under the circumstances to protect client information. For example, Kentucky Bar Opinion E-437 (2014) states:

Because technology evolves every day, we decline to mandate in this opinion specific practices regarding the protection of confidential client information in the world of the cloud. The reality is that such practices soon would be obsolete—and our opinion would be obsolete as well. Rather, we choose to guide lawyers in the exercise of reasonable judgment regarding the use of cloud technology. See Vt. Eth. Op. 2010-6

---

6. See also N.J. Ethics Op. 701 (2006); 2008 N.C. Formal Ethics Op. 5 (2008) (“law firm must enact appropriate measures to ensure that each client only has access to his or her own file [and] that third parties cannot gain access [to] any client file”).
(2010) (constantly changing nature of cloud technology makes establishing “specific conditions precedent” to use not appropriate); Ohio Informal Adv. Op. 2013-03(2013) (“applying existing principles to new technological advances while refraining from mandating specific practices—is a practical [approach]”).

3. Security Precautions That Lawyers Take Need Not Be Infallible; They Must Be Reasonable under the Circumstances

Regardless of whether state bar opinions provide specific guidelines or suggestions as to the appropriate technical safeguards lawyers should take or instead focus on the scope of a lawyer’s obligations to use reasonable care to protect client confidences, it is important to bear in mind that, under the rules of professional conduct, the security measures that lawyers are required to put in place are not required to be invulnerable. As stated in Tennessee Board of Professional Responsibility Formal Ethics Opinion 2015-F-159 (2015):

The lawyer is not required by the rules to use infallible methods of protection. “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. . . . RPC 1.6 Cmt. [16]. . . . Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise affected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality.” Me. Ethics Op. 207 (2013); N.C. 2011 Formal Ethics Op. 6 (2012). “Special circumstances, however, may warrant special precautions.” RPC 1.6, Cmt. [16]. What safeguards are appropriate depends upon the nature and sensitivity of the data. Alaska Ethics Op. 2014-3 (2014).
As illustrated in the above discussion, lawyers cannot take the “ostrich” approach of hiding their heads in the sand and hoping that their office or firm will not suffer a data breach, compromising client information. Lawyers must implement administrative, technical, and physical safeguards to meet their obligation to make reasonable efforts to protect client information.

Furthermore, under ABA Model Rule 1.9(c), this obligation of confidentiality also applies to information about former clients:

A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter: (1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.

B. Competence

In addition to an obligation to keep client communication and sensitive information confidential, a lawyer’s ethical obligation of competence requires that lawyers become and remain competent about the technology they use so as to be able to protect client confidential information.

ABA Model Rule 1.1 states that “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill thoroughness and preparation reasonably necessary for the representation.” One recent change to the ABA Model Rules based on an Ethics 20/20 Commission proposal amended Comment [6] to Rule 1.1, so that it now reads: “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. . . .” (Added language italicized.)

California State Bar Opinion 2015-193 (2015) examined the parameters of a lawyer’s obligations to understand the benefits and risks of technology in the context of e-discovery, stating:
An attorney’s obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

Note especially the second item in the last sentence: If an attorney is not competent to decide whether use of a particular technology (e.g., e-discovery, cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer.

Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject. Arizona Bar Opinion 09-04 (Dec. 2009) reminds lawyers that, if they provide an online file storage and retrieval system for client access of documents, then they must take reasonable precautions to protect the security and confidentiality of client documents and information. With respect to a lawyer’s obligation to be competent, the opinion noted that “[i]t is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.”

Moreover, competence requires continued vigilance and learning, as technology advances, in order to comply with a lawyer’s duties under the ethics rules. Again, the Arizona Bar also reminded lawyers that “[a]s technology
advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.” In other words, lawyers may not assume that their ignorance about technology will be a recognized excuse for their failure to learn, and stay up-to-date, about technology related to a client’s electronically stored information.⁸

C. Supervision of Lawyers and Nonlawyers
Finally, it is not enough that the lawyer is concerned about his individual use of technology and handling of sensitive client information. The ethics rules in every jurisdiction also obligate lawyers to appropriately supervise those who work for them. So, for example, ABA Model Rule 5.1 provides that “[a] partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.”

Similarly, with respect to a nonlawyer employed or retained by or associated with a lawyer, Rule 5.3 provides that “a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person’s conduct is compatible with the professional obligations of the lawyer.”

Lawyers in any supervisory role not only are obligated to follow the ethics rules personally in protecting client confidential information, but must also be vigilant and make reasonable efforts to ensure that lawyers and nonlawyers they supervise adhere to them as well.

These obligations were emphasized and confirmed in the ABA’s latest guidance on this subject, in ABA Formal Opinion 477R, discussed above.

⁸. For further information on lawyers’ ethical obligations of competence when using technology, see ABA Center for Prof’l Responsibility, Ethics Tip: Searching for the Mr. Spock in You (Aug. 2015), http://www.americanbar.org/groups/professional_responsibility/services/ethicsssearch/ethicstipsaugust2015.html (Aug. 2015), and Ethics Tip: Competence: Acquire It or Hire It! (May 2014) http://www.americanbar.org/groups/professional_responsibility/services/ethicsssearch/ethicstipofthemonthmay2014.html.
III. The Law of Lawyering

A narrow focus on a lawyer’s obligation under the law of legal ethics may well lead lawyers and law firms to ignore other related liability that might result from confidentiality breaches. While a breach that results from a lawyer’s failure to comply with her obligations under the ethics rules like ABA Model Rule 1.6 might lead to lawyer discipline, a breach of confidentiality caused by a lawyer’s conduct could well lead to liability to clients and others harmed under other related law, such as malpractice law and fiduciary duty law.

Thus, another source of the obligation of lawyers and law firms to protect against disclosure of confidential information entrusted to them is the common law of malpractice liability and fiduciary duty, as well as traditional statutory remedies available in some jurisdictions for some lawyer misconduct, including laws prohibiting unfair and deceptive trade practices. Despite the novelty of all the new technology involved and the new laws covering this technology discussed elsewhere in this chapter and this Handbook, these traditional causes of action and remedies are just as applicable to a breach of security in the latest cloud-based technology as they are to the loss of a box of paper documents containing confidential client information.9

There can be no doubt that traditional bodies of law used to hold lawyers and law firms accountable for certain harms resulting from their conduct can be used for data and other cybersecurity breaches. With respect to harms suffered by clients, the law offers an obvious path for malpractice liability to a client predicated on a breach of confidentiality and for liability to a client for breach of the fiduciary duty of confidentiality. Inadvertent disclosures of confidential information have, under such principles, led to claims against lawyers and law firms. Of course, intentional misappropriation and misuse of client confidential information can lead not only to claims on these theories, but also to claims under other theories premised upon intentional misconduct, both common law and statutory. Under all

---

9. For treatment of the insurance coverage of the liability of lawyers and law firms under lawyer professional liability theories, see Chapter 15 of this Handbook.
IV. Examples of the Emerging Application of Ethics and Lawyering Law to New Technology

In this section, we review the application of the rules to particular technologies as they have arisen, been adopted by lawyers and their clients, and changed over time. One fundamental principle runs through all of these authorities: when a lawyer decides to use any of these new technologies, the lawyer must have a basic understanding of the technology employed and must take reasonable, prudent steps to preserve client confidentiality, balancing the degree of sensitivity of the information with the need to take additional precautions as appropriate.

A. E-mail

1. To Encrypt or Not to Encrypt?

E-mail was one of the first new types of technology to cause widespread concern in the profession because of perceived threats to client confidentiality. Early in the 1990s, a number of ethics committees issued opinions warning against the use of e-mail to transmit confidential client information, and several of these concluded that a lawyer should not transmit client information through e-mail unless it was encrypted.

As the thinking around e-mail developed, later state bar ethics opinions concluded that an e-mail is similar to a telephone call, and that lawyers have a reasonable expectation of privacy when using it, since it is just as illegal to intercept an e-mail as it is to wiretap a phone call. However, these opinions also stated that lawyers should still exercise caution when using e-mail, just as they would with any other form of communication. If the information is so sensitive that a lawyer would not discuss it over the telephone, chances are that he or she should not use e-mail either.

In 1999, the ABA Standing Committee on Ethics and Professional Responsibility weighed in on this issue in Formal Opinion 99-413,
Protecting the Confidentiality of Unencrypted Email. In language quite similar to the Ethics 20/20 Commission’s later amendments to the comments to Rule 1.6, the committee stated that, if a lawyer has a very sensitive matter to be discussed with a client, he should do it in person. The opinion stated:

The Committee believes that email communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded email transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted email transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including email. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law. . . .

The conclusions reached in this opinion do not, however, diminish a lawyer’s obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of email, just as they would warrant the avoidance of the telephone, fax, and mail.

Immediately before the publication of this edition of the Handbook, the ABA revisited this guidance in its new ABA Formal Opinion 477R, discussed above. This new opinion rejects an overly broad interpretation of earlier Opinion 99-413, which some read to mean that a lawyer was ethically permitted to use unencrypted e-mail for client confidential communications in every circumstance. In formulating guidance for when additional security measures might be needed, the committee looked, among other
129

Lawyers' Obligations to Provide Data Security Arising from Ethics

authorities, to Texas Opinion 648 (2015), which identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

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;
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 National Security Agency or a law enforcement agency may read the lawyer’s email communication, with or without a warrant.10

In a similar vein, Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2011-200 encouraged encryption when using “vulnerable methods of communications”:

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these

devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

2. **Duty to Warn Client When Third Parties May Have Access to Client’s Computer**

ABA Formal Opinion 11-459, Duty to Protect the Confidentiality of Email Communications with One’s Client (2011), addressed the precautions a lawyer should take when he knows that his or her client is using the employer’s computer or other electronic device to communicate with the lawyer. The opinion noted that, under such circumstances, the employer may, as a matter of company policy, have access to the employee’s communication and stated that the lawyer should warn the client about the risks of using such devices:

Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of email communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

State bar opinions have come to similar conclusions.

In ABA Formal Opinion 11-460, the committee addressed in effect the “mirror image” of Formal Opinion 11-459: a lawyer’s ethical obligations upon receiving copies of a third party’s e-mail correspondence with his or her lawyer. As in Opinion 11-459, the committee based its discussion on a hypothetical involving an employee who files an employment discrimination suit against his employer. The employer subsequently copies all of the employee’s e-mails and forwards them to the lawyer. The lawyer
reviews them and finds some correspondence between the employee and the employee’s lawyer that are marked “Attorney-Client Confidential Information.” The committee concluded that, under Rule 4.4, the lawyer would not have an obligation to notify opposing counsel that she had received the information.11

B. Portable Devices and Other Devices That Retain Data
Law firms today use many devices that store confidential client information, including desktop computers, laptops, tablets, printers that store data, flash drives or thumb drives, and cell phones and smartphones. The fact that these devices can store vast amounts of confidential client information mandates that lawyers should take adequate precautions to ensure that the information is protected from disclosure. The extreme portability of some of these devices—smartphones and flash drives come to mind immediately—makes it particularly important for lawyers to use them with thought and care.

But, in recent years, lawyers and others have also learned that danger lurks in devices not ordinarily thought of as likely to retain confidential information. Basic security measures have long included efforts to remove all confidential information from devices before they are disposed of or recycled. More recently, however, press reports that some modern copiers and printers include memory technology that retains images of documents, essentially on a permanent basis, have led many users to understand that disposal of even these pieces of equipment must be accompanied by erasure or removal of memory, just as with the disposal of a desktop computer. For example, Alabama Opinion 2010-2 (2010) states that when disposing of electronic devices, lawyers should ensure that confidential information has been removed. This obligation tracks closely the well-understood obligation of a lawyer to dispose of paper client files in a way that avoids the possibility of disclosure of confidential information (for example, by shredding).

In 2010, the Ethics 20/20 Commission’s Working Group on the Implications for New Technologies suggested possible precautions lawyers should

11. For additional information, see Appendix K (Ethics Opinions on Lawyer Confidentiality Obligations concerning E-mail) of this Handbook.
take when using portable devices, and most of these precautions apply with equal force to any piece of equipment, portable or not, that stores confidential information:

- providing adequate physical protection or having methods for deleting data remotely in the event that a device is lost or stolen;
- encouraging the use of strong passwords;
- purging data from devices before replacement;
- installing safeguards to combat viruses, malware, and spyware;
- erecting firewalls;
- ensuring frequent backups of data;
- updating computer operating systems to ensure that they contain the latest security protections;
- configuring software and network settings to minimize security risks;
- encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them; and
- avoiding public “Wi-Fi hotspots” when transmitting confidential information.12

The ubiquity and ease of use of portable devices carries with it particular problems for lawyers. One common example is the use of laptops and other portable devices away from a lawyer’s regular place of work.

California State Bar Opinion 2010-179 (2010) addressed a situation where a lawyer used a law firm laptop both in a local coffee shop, accessing the Internet using the coffee shop’s Wi-Fi connection, and at his home, using his personal wireless connection. The opinion listed a number of factors for a lawyer to consider when using different types of technologies that have the capability of storing and disseminating confidential client information. These factors include the lawyer’s ability to understand and assess

the level of security offered by the particular technology, how the particular technology differs from other media, whether reasonable steps can be taken to increase the level of security of such technology, and the limitations on who has access to it. The opinion stated that lawyers should also assess the legal consequences to third parties including possible criminal charges or civil claims should they illegally intercept or access the confidential information, as this could affect the extent to which the lawyer using the service or technology could claim a reasonable expectation of privacy. The lawyer should also take into consideration the degree of sensitivity of the information, and the extent to which unauthorized disclosure would adversely affect the client: the greater the sensitivity, the less risk the lawyer should take. Finally, if the client has instructed the lawyer not to use a certain type of technology, the lawyer should abide by the client’s instructions.

Applying these factors to the scenario described in the opinion, the California committee concluded that the lawyer should not use the wireless services offered in the coffee shop unless he had in place adequate safeguards such as wireless encryption and firewalls to protect client information. With regard to use at home of the laptop, the committee stated that the lawyer could use it so long as his home system had adequate security features.

C. Metadata Leaks

Many ethics committees have addressed the application of ethics rules to questions involving metadata—that is, electronic information about electronic documents that is often associated with, or a part of, the document, but often not readily visible to the ordinary user. The question most frequently addressed, however, is whether a lawyer who receives a document containing metadata (for example, a Word file containing a document being negotiated between the lawyer’s client and someone else) may ethically look for and review that metadata, as the metadata may well contain useful, otherwise confidential information.

While those opinions reflect varied opinions on whether the receiving lawyer may or may not look for and review metadata, a number of ethics opinions address the related question: What obligation does a lawyer have to protect against the disclosure of metadata that reveals confidential information of his or her client? The authorities that do address this question
apply the same analysis for the protection from disclosure of metadata as for ordinary data—a lawyer must take reasonable precautions to avoid disclosure of confidential client information, in whatever form.13

D. Outsourcing

Outsourcing is another area where confidential client information is subject to cybersecurity threats. When a lawyer engages an outside service provider to provide legal or law-related services for his or her clients, and allows the provider access to confidential client information, the lawyer must ensure that the outside entity has in place reasonable safeguards to protect against unauthorized disclosure. If the service provider is a legal professional outside of the United States, the lawyer may well have an obligation to ascertain whether the laws and professional conduct rules of the foreign jurisdiction share the same basic core values of client confidentiality.

The latest revisions to the ABA Model Rules of Professional Conduct, based on 2012 proposals from the Ethics 20/20 Commission, address a lawyer’s obligations concerning outsourcing. These amendments codified, to a great extent, a 2008 ABA ethics opinion on this subject in amendments to comments to Rule 1.1 and 5.3.

The commission proposed amendments to the comments to Rules 1.1 and 5.3 on how to supervise and select outside service providers that have in place adequate measures to protect client information. New Comment [6] to Rule 1.1 states:

Retaining or Contracting with Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer’s own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers’ services will contribute to the competent and ethical representation of the client. . . . The reasonableness of the decision to retain or contract with

13. For additional information, see Appendix L (Ethics Opinions concerning a Lawyer’s Obligations to Prevent the Inadvertent Disclosure of Confidential Client Information in Metadata).
other lawyers outside the lawyer’s own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

In 2008, the ABA Standing Committee on Ethics and Professional Responsibility addressed a number of these issues relating to confidentiality in its Formal Opinion 08-451, Lawyer’s Obligations When Outsourcing Legal and Nonlegal Support Services.

The opinion considered outsourcing in a wide variety of contexts, such as the use of contract or temporary lawyers, photocopy shops or information technology vendors, legal research services, or foreign lawyers to draft patent applications. Among the lawyer’s duties implicated by the use of such outsourcing, the opinion noted, are the duty of competence (Rule 1.1) and the duty to supervise (Rules 5.1 and 5.3). The committee offered the following suggestions to help the outsourcing lawyer comply with the duties of competence and supervision:

- Conduct background checks of any lawyer, nonlawyer, or placement agency involved;
- Interview the principal lawyers involved, and assess their educational backgrounds;
- When working with an intermediary, inquire into its hiring practices so as to ascertain the character of the employees who are likely to have access to client information;
- Investigate the security measures in effect in the provider’s premises, including its computer network and refuse disposal systems;
- Depending on the circumstances, consider conducting an on-site visit in order to get an impression of the professionalism of the lawyers and nonlawyers involved.

The committee stated further that when the work will be outsourced to a foreign country, the outsourcing lawyer should also ascertain whether the
legal training received in that country is comparable to that in the United States, whether legal professionals in that country share the same core ethical principles with lawyers in the United States, and whether there is an effective professional discipline system. If the legal professionals’ legal system does not share the same core principles or does not have an effective lawyer discipline system, the outsourcing lawyer would have a heightened duty to scrutinize the work produced, and may have an obligation to disclose to the client the risks associated with having the work outsourced to that country.

The opinion also particularly highlighted an outsourcing lawyer’s duty to protect client confidentiality, including by taking reasonable measures to protect confidential information necessarily disclosed in the course of the outsourcing, for example, by using confidentiality agreements to bind vendors contractually to protect client information. Further, the outsourcing lawyer who uses foreign vendors will need to evaluate the protection afforded the client’s confidentiality by the foreign jurisdiction.

In a like vein, an earlier opinion, ABA Formal Opinion 95-398, Access of Nonlawyers to a Lawyer’s Data Base (1995), had addressed the ethical implications of allowing a computer maintenance company to have access to a law firm’s computer network. The opinion stated that the law firm could allow access so long as it took steps to ensure that it had in place adequate security measures to protect confidential client information.14

E. Cloud Computing

“Cloud computing” can describe any system whereby a lawyer stores digital information on servers or systems that are not under the close control of the lawyer or the lawyer’s firm.15

A lawyer’s use of cloud computing can be both economical and beneficial, but as many state bar ethics opinions have noted, lawyers who use “the cloud” must take steps to ensure that confidential client

---

14. For additional information, see Appendix M (Ethics Opinions on Lawyer Confidentiality Obligations concerning Outsourcing).

15. Additional discussion about the technical aspects of cloud computing can be found in Chapter 3 of this Handbook.
Lawyers’ Obligations to Provide Data Security Arising from Ethics

information that is placed there is adequately protected from disclosure. Many opinions suggest a number of factors to use in assessing whether the protections are adequate, but with the proviso that rapidly evolving technology means that these factors cannot provide a “safe harbor.” Lawyers should monitor and reassess the protections of the cloud provider as the technology evolves.

As an example, Illinois State Bar Advisory Opinion 16-06 (2016) suggested the following steps lawyers should consider taking when deciding whether to engage the services of a cloud computing provider:

1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
3. Investigating the provider’s reputation and history;
4. Inquiring whether the provider has experienced any breaches of security and if so, investigating those breaches;
5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer’s duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
6. Requiring that all data is appropriately backed up completely under the lawyer’s control so that the lawyer will have a method for retrieval of the data;
7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.

Opinions addressing cloud computing also make clear that a lawyer must have a basic understanding of the technical aspects of cloud computing, and should conduct a due diligence evaluation of the provider to ensure that it has adequate security measures. As Washington State Bar Opinion 2215 points out, ignorance of technology is no excuse for the failure
to conduct such an investigation. A lawyer who does not understand the technology or whether it is sufficiently secure for use should consult with someone who does.\textsuperscript{16}

In order to determine whether a lawyer has made “reasonable efforts” to ensure that outside vendors who provide communications technology have taken appropriate steps to protect client confidences, the ABA’s new Formal Opinion 477R suggests a number of factors for evaluating technologies and vendors that are very similar to those identified by the many state bar ethics opinions on cloud computing.

F. Social Media

1. Lawyers and Social Media

Social media networks such as Facebook, Twitter, and LinkedIn have grown exponentially over the past several years. Though lawyers have been slower than the general public and other businesses to adopt social networks, their use is becoming more and more prevalent among lawyers. While the use of social media networks may pose various risks for lawyers and others, for purposes of cybersecurity for lawyers and law firms, the questions about these networks revolve around confidentiality and lawyers’ understanding of the technology that drives them.

The strong tendency on social networks for users, including lawyers, to share information, combined with the blurred distinctions between a lawyer’s personal and professional activities, opens the possibility that client confidential information may be shared by a lawyer, perhaps without careful deliberation. Of course, the lawyer’s confidentiality obligations do not stop when the lawyer is logged on to social media. Moreover, the increased sharing of information among a wide range of people (sometimes including people not known to the lawyer using the service) may lead to the disclosure of seemingly innocuous information that may somehow reveal confidential client information (for example, the mergers and acquisition lawyer’s plans for travel to a city in which a particular business is located).

\textsuperscript{16} For additional information, see Appendix N (Ethics Opinions on Lawyer Confidentiality Obligations concerning Cloud Computing).
Even when social networks are, in fact, used by lawyers for professional purposes—for example, posting a query to other lawyers about a knotty procedural problem in a pending case—the risk of disclosing client confidential information exists. In ABA Formal Opinion 98-411 (1998), Ethical Issues in Lawyer to Lawyer Consultation, the ethics committee addressed lawyer-to-lawyer consultations of a similar type:

The consulting lawyer should not assume, however, that the anonymous or hypothetical consultation eliminates all risk of disclosure of client information. If the hypothetical facts discussed allow the consulted lawyer subsequently to match those facts to a specific individual or entity, the information is not already generally known, and disclosure may prejudice or embarrass the client, the consulting lawyer’s discussion of the facts may have violated his duty of confidentiality under Rule 1.6.

The sweeping reach of client confidentiality under ABA Model Rule 1.6—which requires protection of all “information relating to the representation,” from whatever source—and under the rules in most jurisdictions counsels great care on the part of lawyers in sharing information that may touch on their professional lives. Further, just as with any other technology, lawyers have an obligation to be knowledgeable enough about any social network they use such that they can appropriately protect client confidentiality.

Moreover, a lawyer’s duty to supervise other lawyers and nonlawyers may include educating them concerning how their confidentiality obligation applies even among “friends” on Facebook and alerting them that “casual” comments made on LinkedIn after a difficult hearing may be risky. Rules 5.1 and 5.3 on supervision may also require that a lawyer or law firm have in place internal firm policies designed to protect client confidences in this context. These rules do require that lawyers who manage their own practices or their firms must make sure they have in place “measures giving reasonable assurance that” obligations under the ethics rules, including confidentiality obligations, are met.
It is common practice to post the minutiae of daily life on social media sites. However, when lawyers post information about their clients, they confront the broad reach of Rule 1.6 that protects from disclosure all information relating to the representation without client consent, unless impliedly necessary to carry out the representation, or unless another exception listed in Rule 1.6(b) applies. Even a post that refers to a client matter that is redacted to remove any identifying information can be a breach of confidentiality if someone who reads the post could reasonably ascertain to whom the lawyer is referring and what the matter is about.17

2. Passive Communications with Jurors
As with all forms of technology, it is vitally important that lawyers understand the consequences of certain technical features of social media. To illustrate, consider the body of ethics opinions and court rules that have arisen over issues involving “passive” communications with jurors on social media.

While it is common practice for trial lawyers preparing for voir dire to search the Internet to acquire information about potential jurors, some jurisdictions have found such investigation to be inappropriate to the extent that the juror becomes aware that he or she is being monitored. Based on some of these opinions, the ethical propriety of the lawyer’s conduct may depend on the functionality of the social media network.

On some social media networks, the network alerts a user where someone else views or visits the user’s page or profile; on other social media networks, a user may have no idea of the identity of someone (such as a lawyer doing investigation for purposes of voir dire) viewing the user’s page or profile. Indeed, on some social networks, whether a user is alerted to such viewing or the identity of the viewer may depend on how the viewer accesses the network or even the settings of the user or the viewer. Knowing these details of the functionality of the particular social media network may well be crucial for a lawyer deciding whether and how to ethically investigate potential jurors.

17. See Appendix O (Ethics Opinions Relating to Lawyers’ Passive Communications with Jurors on Social Media).
ABA Formal Opinion 466, Lawyer Reviewing Jurors’ Internet Presence (2014), addressed this issue and concluded that this was not a communication from the lawyer to the juror since it was the social media platform and not the lawyer that initiated the notification to the juror, analogizing the situation to that of a neighbor who reports to the juror that he saw the lawyer’s car driving down the juror’s street.

The committee cautioned, however, that lawyers should educate themselves about the features of the different social media platforms sites and that “lawyers who review juror social media should ensure that their review is purposeful and not crafted to embarrass, delay or burden the juror or the proceeding.”

Earlier opinions from New York appeared to reach different conclusions, stating that notifications received by jurors from their social media website that the lawyer had visited their site had the potential to harass and intimidate the juror and constituted an impermissible communication with a juror in violation of Rule 3.5. In view of this potential to run afoul of Rule 3.5, these opinions cautioned that lawyers have an obligation to familiarize themselves with the features of a particular social media platform so as to avoid any inappropriate communications with a juror.18

V. Conclusion

We lawyers, like our clients, live and practice in a rapidly changing communications and technology environment, and there is no end in sight for these changes. Over the last 20 years, culminating in the ABA’s recent Opinion 477R, our ethics rules have been interpreted to provide guidance as to how we can discharge our ethical obligations in a time when threats, technology, security vulnerabilities, and protection measures available, as well as their relationships one to another, are also dynamically changing.

Whether it be cloud computing, the use of unencrypted or encrypted e-mail, participating in social media, or the use of the latest electronic gadget, lawyers have an obligation to make reasonable efforts to protect their

client confidential information. What is found to constitute “reasonable efforts” will depend on a number of factors including “the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed,” and the cost and difficulty of implementing them.

Applying these factors, ABA Formal Opinion 477R informs us that when transmitting client information over the Internet, encryption should be considered as an additional security safeguard when warranted by the circumstances.

Lawyers also have an obligation to understand the benefits and risks associated with these new technologies. If for any reason they are unable to do so, they should consult with someone who does.

Lawyers who supervise other lawyers and nonlawyers also have a duty to make reasonable efforts to ensure that their conduct conforms to the rules of professional conduct and that they follow appropriate security procedures to protect client confidences.

Following are the top ten ethical and other considerations with respect to lawyer obligations to protect client data:

1. A lawyer should acquire a basic understanding of the “benefits and risks associated with relevant technology” used in his or her day-to-day practice. A lawyer who does not have such an understanding should identify and consult with someone who does.

2. Technology is a moving target. Keeping current about changes in technology is an ongoing process. A lawyer must continually reassess and evaluate security measures as new technologies develop and come into use by lawyers and their clients.

3. Be aware that the scope of the information protected under the ethics rules—ABA Model Rule 1.6—is very broad. It includes all information relating to the representation.

4. Be mindful of obligations to protect a former client’s confidential information (under Model Rule 1.9(c)) as well.

5. When using technology to either store or transmit information, lawyers must make reasonable efforts to prevent the inadvertent disclosure of or unauthorized access to confidential client information.
6. Reasonable efforts to prevent the inadvertent disclosure of or unauthorized access to confidential client information include assessing the sensitivity of the information and the likelihood of disclosure if additional safeguards are not employed. Depending on the circumstances, encryption may be an appropriate additional security safeguard.

7. In an office or firm, have in place procedures by which both lawyers and nonlawyers are trained and monitored in their use of technology to ensure that client confidences are protected.

8. When disposing of portable electronic devices, take precautions to ensure that all confidential client information has been removed. If the devices are recycled, verify that the recycler follows appropriate protocols to remove the data.

9. When transmitting electronic documents to third parties, remove metadata that contains confidential client information.

10. When using cloud computing or outsourcing services, verify that the service provider has in place adequate security measures to prevent the inadvertent disclosure of or unauthorized access to confidential client information.
Abstract

Sweeping advances in technology are not only changing the law that attorneys practice, they are also causing profound changes to the way attorneys practice law. For instance, the combination of consumer-friendly mobile devices and cloud computing means that attorneys now have the technology to access all their work data with any device, at any time, and anywhere in the world, as long as they have an Internet connection. Nonetheless, new technologies create new threats to the confidentiality of client data.

Ethics rules impose duties on attorneys to protect client confidences. They also require attorneys to practice competently and to supervise office staff and third parties with access to client data. The operation of these rules will require attorneys and law firms to implement reasonable information security practices to protect the confidentiality, integrity, and availability of client data. The failure to protect client data may lead to attorney discipline or malpractice liability. Solo lawyers and small firms are subject to the same rules as large firms. Consequently, they cannot ignore information security requirements.

Moreover, information security is not just a “technology issue” that can be delegated without supervision to information technology support staff. Attorneys themselves have an obligation to manage and oversee the security function in their firms. Lessons learned from other industries and industry standard security frameworks can help law firms implement effective security programs. We present a set of sample security safeguards that solos and small firms can use to implement administrative, physical, and technical safeguards to protect client data.
I. **Introduction**

With advancing computing technology, we live in an era of unprecedented computing power and connectivity. Modern computing devices have as much power as mainframe computers running entire government agencies in the 1960s. Desktop and laptop computers are standard equipment for modern knowledge workers. Workers frequently telecommute by using their laptops or home computers.

Moreover, mobile device usage is now a way of life. Walking around our cities and towns, it seems that everyone has a smart phone in hand. In the office, at home, and in planes, trains, and automobiles, people are communicating, writing, and doing their work using smart phones, tablets, and laptops. Besides offering us voice, email, and text communications on the go, our mobile devices are giving us access to the world's information via the Mobile Internet more or less anytime and anywhere. If a law firm’s systems are connected to the Internet, technology enables today’s lawyer to obtain access to client data at any time from any device from any place in the world with Internet or cellular connectivity.

With these advances in technology, information security threats have increased. Data breaches continue to be an everyday occurrence. We see them in the news all the time. Competitors, former employees, and state-sponsored groups seek companies’ trade secrets in order to bolster competing businesses. Hacktivist groups seek to damage the reputation of companies by publicizing sensitive information. Organized crime rings seek sensitive information for profit.

Law firms are not immune from attacks. For instance, in 2011, a Chinese hacker group gained unauthorized access to the systems and data of Wiley Rein LLP in Washington D.C. Wiley had pursued unfair trade claims against exporters in China and, in just one case, obtained tariffs on more than $3 billion in exports of solar cells. The Chinese hacking group not only penetrated the firm’s networks, it stole large amounts of data.

---


from a various entities, including the president of the European Union Council, Haliburton Co., and a Canadian magistrate.\textsuperscript{3}

One FBI agent put it succinctly: “Computer attacks on law firms happen every day . . . .”\textsuperscript{4} Many of these attacks fail, but some succeed. The bottom line is, “Many large law firms have been hacked; the FBI has warned that law firms are being targeted.”\textsuperscript{5} We, as attorneys, are on notice of the threat.

More recently, “Petya” malicious software, a kind of “ransomware,” attacked international firm DLA Piper in June 2017 and brought the firm’s information technology infrastructure to its knees.\textsuperscript{6} Ransomware is a kind of malicious software that attacks systems by encrypting a user’s or network’s files and displaying a screen demanding a payment of ransom to obtain a key to decrypt and recover the user’s or firm’s data. For DLA Piper, old emails and files were unavailable more than two weeks after the attack, and the lost business and recovery costs were probably in the millions of dollars.\textsuperscript{7}

Moreover, ransomware and other malicious software attacks are not limited to large law firms. Although the most publicized breaches involve large law firms, and we do not have large, comprehensive surveys about exact numbers, our discussions with security professionals lead us to believe countless numbers of small firms have been victims of attacks as well. The loss of an entire practice’s worth of data may be more devastating to that small firm than a similar attack against a large firm. A large firm may have in-house and retained expert technical support, the resources to fund data recovery operations, and the ability to recover data after perhaps weeks in the case of DLA Piper. For some solos and small firms, the attorneys may never be able to recover their client data and may have to start their electronic recordkeeping from scratch.


\textsuperscript{5} Interview with Rhodes and Polley, \textit{supra}.


\textsuperscript{7} See Jonathan Crowe, How One of the World’s Largest Law Firms Was Paralyzed by Petya (Jul. 2017), \url{https://blog.barkly.com/dla-piper-petya-ransomware-attack}. 
In addition to anecdotal evidence, one survey of 200 small and medium sized firms found a general lack of risk management mechanisms and procedures. Among the key findings were:

- Most firms in the survey are not implementing key security controls
- Almost half of the respondents don’t have formal security policies and procedures or a documented training program.
- Most firms don’t have response plans or backup procedures in place.

The ABA, recognizing increasing cyber threats, adopted a House of Delegates resolution calling for “all private and public sector organizations to develop, implement, and maintain an appropriate security program.” The report accompanying the resolution made it clear that the resolution covers law firms and legal services organizations. This resolution followed an earlier 2012 House of Delegates resolution proposed by the Commission on Ethics 20/20 approving changes to the ABA Model Rules of Professional Conduct. The resolution amended the Model Rules to impose a duty on lawyers to use reasonable efforts to prevent unauthorized access to client data and made related changes to address the advances of technology. The ABA has also created a number of publications to help lawyers and law firms improve their information security programs.

In 2012, the ABA created a Cybersecurity Legal Task Force. The Task Force’s mission is to “identify and compile resources within the ABA that pertain to cybersecurity, and will focus and coordinate the ABA’s legal and policy analyses and assessments of proposals relating to cybersecurity.” The most important output of the Task Force was

---

9 Id. at 4-5.
11 Id., Report at 1 & n.1.
its comprehensive cybersecurity guidance book for lawyers and law firms in 2013; the ABA issued a second edition of the book in 2018.14

II. Information Security Risks to Law Firms

Law firms are recognized targets for attack for a number of reasons. First, law firms have large amounts of information that would be valuable to state or non-state actor attackers. “They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.”15 For instance, attackers might want to steal trade secrets about a firm client in order to gain an advantage in the marketplace. Moreover, attackers may be interested in the identity of potential acquisition targets in order to profit by the information via stock trades.16 Also, some firms hold personal information about individuals, whether clients or opponents, that could be used for identity theft purposes, such as names, birthdates, and social security numbers.

Second, law firms are perceived as easy targets for attacks. Attackers seeking information about a particular company may find it easier to find out the identity of the law firms representing it, and to try to attack the law firms' systems, than to attack the company's systems directly. Law firms are “perceived to have fewer security resources than their clients, with less understanding of and appreciation for cyber risk.”17 Finally, a hack against a law firm may be more efficient and save time, compared to an attack against a firm client. “[L]awyers are usually involved in only their client’s most important

business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information.”

Threats to law firms may arise from a number of sources. For instance, some law firms may fall victim to malicious insiders. Malicious insiders may be motivated by job dissatisfaction or may seek to compromise client data for financial gain. For instance, in 2001, a paralegal at a large firm in New York downloaded a copy of a trial plan from his firm’s computer system and tried to sell the plan to opposing counsel for $2 million. Fortunately for the firm, the scheme was exposed and the paralegal made the sale to an undercover FBI agent. He eventually pleaded guilty to Computer Fraud and Abuse Act violations, wire fraud, and related charges. Some insiders may also have political or social activism motives.

State-sponsored attacks are another source of information security threats. State actors may be motivated by economic espionage, terrorism, or politics. Foreign or domestic criminal enterprises may seek information to sell or use in order to make money. Non-state “hacktivists” may hope to achieve a political objective through attacks. Terrorists may make hacking attacks both for profit and to terrorize their victims. Finally, business competitors sometimes seek information about other companies in their markets using extra-legal techniques.

Given these increasing threats, our clients are now asking law firms about their security programs and are seeking written assurances of security as a condition of giving business to their outside counsel. For instance, “Wall Street banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and deter attacks from hackers bent on getting their hands on corporate secrets either for their own use or sale to others . . . .”

A law firm’s failure to protect client data may cause considerable damage. “Clients and third parties may find themselves victims of fraud, identity theft, and bankruptcy, not to mention negative publicity and tarnished business reputation.” Following a breach, a

---

18 Id.
20 Cybersecurity in Our Digital Lives, supra, at 129.
22 Cybersecurity in Our Digital Lives, supra, at 129.
law firm’s clients or third parties could incur liability in civil actions, administrative proceedings, or even criminal charges. Attorneys or law firms that fail to protect data may face discipline from their state bars, government investigations, fines, private law suits, and malpractice claims by clients. In fact, in 2016, a putative class of clients filed a malpractice suit against a law firm alleging that the firm’s time tracking web-based application used out of date supporting server software, the application was thus insecure, and the firm thereby put client data at risk. Although the case ended in an order compelling arbitration, we expect that the firm filing this action, Edelson PC, is continuing to look for other opportunities to assert claims against law firms with vulnerable or hacked systems. Most importantly, a data breach may cause considerable harm to the reputation of a hacked law firm and its lawyers. Clients, judges, the legal community, and members of the public may lose trust in the firm. If sufficiently serious, a data breach could be a threat to the very survival of a law firm.

III. Attorneys’ Ethical Obligations to Protect Client Data

Lawyers and law firms have ethical obligations under the rules of professional conduct in their jurisdictions. The ABA published and regularly updates the ABA Model Rules of Professional Conduct. States have their individual ethical rules, although most are based on the ABA’s Model Rules. As mentioned above, the ABA Commission on Ethics 20/20 proposed changes to the Model Rules based on their evolving views about the impact of technology on the practice of law. The House of Delegates passed a resolution approving these changes. Various ABA opinions provide additional guidance on security issues.

23 Id.
24 Shore v. Johnson & Bell, No. 16-cv-4363 (N.D. Ill. complaint filed Apr. 15, 2016).
26 Cybersecurity in Our Digital Lives, supra, at 129.
State ethics opinions provide an additional source of guidance for understanding attorneys’ ethical obligations under their rules. In addition, secondary sources of information are available for guidance. In 2006, the ABA Section of Science & Technology Law published a book on law office security. In 2013, moreover, the ABA published The ABA Cybersecurity Handbook, which the ABA updated with a second edition in 2018.

The following sections discuss the core duties under the ethics rules bearing on information security: the duty of confidentiality, the duty of competence, and the duty to supervise.

A. The Duty of Confidentiality

The most important ethical rule relating to lawyer and law firm information security is the duty to protect the confidentiality of client confidences. In general, under ethical rules, “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” The ABA Cybersecurity Handbook explains that “[t]his obligation to maintain confidentiality of all information concerning a client’s representation, no matter the source, is paramount,” and “is no less applicable to electronically stored information than to information contained in paper documents or not reduced to any written or stored form.” Confidentiality is a “core” obligation of a lawyer in the conduct of the lawyer's practice.

Following the ABA resolution in the wake of the work of the ABA Commission on Ethics 20/20, ABA Model Rule 1.6 Part (c) now says that “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” In addition, and perhaps most significantly, Comment 18 now elaborates that “[f]actors 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

30 See generally ABA Cybersecurity Handbook, supra.
31 Model Rules of Prof'l Conduct R. 1.6(a) (Am. Bar Ass’n 2018).
32 ABA Cybersecurity Handbook, supra, at 118.
34 Model Rules of Prof'l Conduct R. 1.6(c) (as amended).
which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”

The Ethics 20/20 Commission’s work was intended to address a lawyer’s obligations in the face of changing technologies. Although not specifically calling out the concept of information security, the Commission’s language is similar to the language in information security legislation. The requirement to protect client data is, in essence, an information security obligation. Commentators have noted the significance of this change, and the new affirmative duty of care for securing client data.

The rules do not specify requirements for the exact security measures necessary in any given situation, such as an attorney-client communication. Indeed, the rules contemplate that the lawyer and client will discuss and then decide what security is necessary. “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.”

Model Rule 1.4 also requires attorney-client communications, specifically “about the means by which the client’s objectives are to be accomplished.” In other words, attorneys should keep their clients reasonably informed about their work together. By implication, this rule requires communication about the law firm’s technology for communicating with clients. Likewise, these rules require a notification in the event of a data breach that compromises client data. ABA Formal Opinion 483 cited Rule 1.4 to state that when a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have an ethical duty to notify current clients of the breach. Lawyers may also have statutory duties to inform clients of data breaches, depending on the type of information compromised and applicable laws.

35 Model Rules of Prof’l Conduct R. 1.6 comm. [18] (as amended).
36 See, e.g., Will Harrelson, Mobile Device security for Lawyers: How Solos and Small Firms Can Ethically Allow Bring Your Own Device, Curo Legal, June 24, 2014, http://www.curolegal.com/mobile-device-security-lawyers-solos-small-firms-ethically-allow-bring-your-own-device/ (“This is a monumental change that sets a new standard suggesting that lawyers are required to implement reasonable technological safeguards to prevent even an ‘inadvertent’ disclosure of a client’s information or data.”).
37 Model Rules of Prof’l Conduct R. 1.6 comm. [19] (as amended).
38 Model Rules of Prof’l Conduct R. 1.4(a)(2).
39 Reis, supra, at 2.
40 Id.
B. The Duty of Competence

In order to maintain client confidences, lawyers must be competent and must keep abreast of changes in information technology they are using in their practices. They cannot protect client confidences unless they know of the nature of the technology they are using, the threats to that technology, and the use of safeguards to mitigate risks. “A lawyer shall provide competent representation to a client.”

“Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. Competence includes the knowledge of substantive law and specific skills, such as knowledge of applicable law, advocacy, writing, and negotiation, but it also includes competence in using the technologies commonly used for law practice.

A lawyer does not need to personally have all the needed technology competencies. The lawyer can, and indeed must, turn to the expertise of staff or outside experts when needed. According to The ABA Cybersecurity Handbook, “If an attorney is not competent to decide whether use of a particular technology (e.g., e-discovery, cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer.”

Nonetheless, a duty of competence means that the lawyer cannot simply turn over all aspects of the security function to others. All workers at the firm have control over certain aspects of their client work and must maintain secure work practices. For instance, attorneys have control over what they talk about in public. They have a duty not to discuss confidential client matters in public places. This is a concern of the attorney, and not just the staff.

---

42 Model Rules of Prof’l Conduct R. 1.1.
43 Id.
44 Model Rules of Prof’l Conduct R. 1.1 comm. [8] (as amended) (emphasis added).
45 Reis, supra, at 2 (“[Model Rule 1.1] requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise.”); ABA Cybersecurity Handbook, supra, at 124 (“Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject.”).
46 ABA Cybersecurity Handbook, supra n. 3, at 124.
Similarly, attorneys must protect paper records. They should not read sensitive paper documents in places where others can view them, such as on the plane or in coffee shops. Again, this is an attorney responsibility.

In addition, lawyers can control their use of technology. For instance, the careless use of social media can lead to compromises of client data. Preventing careless social media usage by lawyers is not a “tech issue” to be handled only by staff.

C. The Duty to Supervise Staff and Third Parties

Lawyers in a law firm must supervise junior attorneys, support staff, and third parties with access to client data. Under the ABA Model Rules, lawyers “shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that,” first, “all lawyers in the firm conform to the Rules of Professional Conduct,” and second, that the conduct of a non-lawyer employed by, retained by, or associated with the lawyer, “is compatible with the professional obligations of the lawyer.” Moreover, in the future, as lawyers and law firms delegate some lawyering tasks to autonomous automated data processing, machine learning, and artificial intelligence systems, these rules will, in our opinion, need guidance from state bar authorities, or even amendments, to clarify that lawyers’ responsibility for the firm includes a duty to supervise these non-human systems as well.

Again, the ethical obligation of the lawyer is to maintain ultimate responsibility for the security function in his or her practice. This is not a duty that can be delegated to others. To the contrary, the lawyer must oversee subordinate attorneys, support staff, third parties, and automated systems.

One specific issue that has come up in the context of supervision is whether a law firm may ethically use cloud computing services to store, share, use, and communicate client data. While a thorough discussion of choosing and supervising cloud service providers is beyond the scope of this paper, ethics opinions have stated generally that cloud computing is permissible, as long as lawyers take proper steps when selecting and using services. For example, in 2013, an Ohio opinion acknowledged that lawyers may use cloud services as long as they competently select an appropriate

\[47\] Model Rules of Prof’l Conduct R. 5.1(a).
\[48\] Id. R. 5.3(a).
\[49\] See ABA Cybersecurity Handbook, supra, at 137 (explaining that state ethics opinions “make clear that a lawyer must have a basic understanding of the technical aspects of cloud computing, and should conduct due diligence evaluation of the provider to ensure that it has adequate security measures”).

Ethics opinions recognize the limitations of lawyers’ competencies. As the New Hampshire Bar has stated, “a lawyer’s duty is to take reasonable steps to protect client data, not to become an expert in information technology,” and “[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard.”\footnote{Barkett, supra, at 10 (quoting New Hampshire Bar Ethics Op. #2012-13/4).} The ABA Cybersecurity Handbook notes that “rapidly evolving technology means that these factors cannot provide a ‘safe harbor.’”\footnote{ABA Cybersecurity Handbook, supra, at 137.} Instead, “[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves.”\footnote{Id.}

IV. Implementing an Effective Information Security Program: the Solo and Small Firm Perspective

The upshot of the ethics rules is that a lawyer must make “reasonable efforts” to prevent inadvertent or unauthorized disclosure of client data, and to prevent unauthorized access to client data.\footnote{Model Rules of Prof’l Conduct R. 1.6(c).} Nonetheless, the rules don’t say what “reasonable efforts” are or what specific safeguards are necessary. How much security is enough under this standard? What is “reasonable”? The factors listed in Section III.A above (such as the level of sensitivity of the client data, risks to data, cost of safeguards, etc.) provide guidance, but they don’t provide ideas to develop specific security safeguards for a security program.


Some states provide more specific requirements. For example, Maine lists seven requirements “the attorney should ensure that the vendor of cloud computing services or hardware” follows. Maine Board of Bar Overseers Opinion #207. The Ethics of Cloud Computing and Storage, http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=478397&v=article.
The issue of what is reasonable is especially acute for solos and small law firms. On one hand, the ethical rules apply equally to small and large practices. On the other hand, compared to larger firms, solo and small firm practices have fewer resources to manage a security program. They don’t have large budgets to spend on information technology and security. Further, small practices won’t usually have a knowledgeable security professional on staff. Larger firms can afford to hire an information security director and may have an in-house team to oversee security. Lawyers and staff in smaller practices may not have the expertise to manage a security program effectively.

For small practices, the good news is that the rules are flexible enough to accommodate the differing circumstances of small practices. As mentioned above, in considering measures to protect the confidentiality of client data, the practice can consider “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).”Thus, the rules allow small practices to account for the cost and difficulty of implementation in deciding what safeguards are reasonable. They do not require small practices to spend all their income on security safeguards; that would not be “reasonable.” The expectations for security safeguards in a solo practice are much different from those for the largest megafirms. Some expensive, difficult-to-implement security measures appropriate for a megafirm are not reasonable for small practices and therefore not required.

In essence, there is a sliding scale of “reasonableness” for small versus large practices. Small law firms can and should implement security safeguards that are reasonable and appropriate to the context of their small size. A full listing of all the security safeguards a law firm could implement is beyond the scope of this paper. The other Cybersecurity panel speakers will be presenting ideas for specific safeguards that a law firm could implement. The secondary sources, such as The ABA Cybersecurity Handbook, also present safeguards a law firm can implement. Nonetheless, this section provides what we believe are practical, concrete, and reasonable examples of security safeguards a small practice can realistically implement. The list is not meant to be exhaustive.

The list breaks down security safeguards into three categories: administrative, physical, and technical safeguards.

- Administrative safeguards create procedures for operating the security function in the firm, focusing on the steps the firm takes to secure client data and how the firm manages the people working at the firm.

55 Model Rules of Prof’l Conduct R. 1.6 comm. [18] (as amended).
Physical safeguards protect the office setting and tangible items comprising or storing client data, including paper records, workstations, mobile devices, portable electronic media, and any servers.

Technical safeguards are the computer- and network-related security mechanisms implemented using software, hardware, and networks, and how people and devices interact with them.\(^{56}\)

Small practices should conduct their own security assessment and review the safeguards in this section. If they don’t have the knowledge to conduct an assessment themselves, they should obtain qualified help. They should consider which safeguards are reasonable and appropriate in light of their individual practices. Following this assessment, they should implement the safeguards they consider reasonable and appropriate.

Different small practices will come to different conclusions about what is reasonable and the details of how to implement different safeguards. For instance, solo practitioners with no support staff will be different from a ten-lawyer firm with support staff. The solo in this example needs no separate responsible person for managing the security function. The solo does everything. Moreover, the solo will be focusing on software for a single individual’s set of devices and can use consumer versions of security software suites and "endpoint" security packages. The term “endpoints” in data security jargon refers to the computers and mobile devices an individual user would use. By contrast, the ten-lawyer firm with support staff is large enough to have centralized management of some computer and network functions and may make use of “enterprise” (company-wide) versions of endpoint security software.

Small firms with a handful of lawyers with enough sophistication to manage their own devices may be able to operate like the solo in our example. But small firms with more lawyers and staff, or those without professionals having the expertise to manage their own devices, will likely find it useful to have a lawyer or staff member to centrally manage some of the technology functions of the firm.

With these caveats in mind, here are examples of administrative, physical, and technical safeguards of typical small practices to protect client data.

\(^{56}\) For a more thorough discussion of these three types of safeguards, see ABA Cybersecurity Handbook, *supra*, at 63.
A. Examples of administrative safeguards:

1. The practice has written policies, procedures, guidelines, and training materials to govern the security function. The practice communicates these policies to individual users.

2. The practice undertakes a risk assessment and updates it at least annually to determine the threats to its client data in light of the sensitivity of the information.

3. The practice follows up with its risk assessment by implementing safeguards that manage its risk to a reasonable level. It should start with the easy, inexpensive controls with the most protective benefits and continue from there to implement more expensive safeguards. Eventually, the practice will reach a point where it has implemented the reasonable safeguards and additional safeguards would not be worth the added expense.

4. The practice has designated a person or team to be in charge of information security. The practice obtains the help of outside consultants as needed to provide additional security management expertise.

5. The practice investigates the background of new hires with access to client data to provide assurances that they are trustworthy and competent.

6. The practice manages which lawyers and staff have access to which kinds of information and change such access when job duties change.

7. The practice has a program of security and privacy awareness and training, including periodic reminders and updates. Topics include the protection of electronic information, controlling access to computer systems, preventing ransomware and other malicious software, phishing risks, social media practices, the protection of paper records, and not discussing client matters in public places.

8. The practice has employment procedures by which lawyers and staff are evaluated in part based on their compliance with security policies and procedures. Lawyers and staff face discipline if they violate those policies and procedures.

9. The practice has procedures for when a lawyer or staff member leaves the practice to stop the departing user’s access to client data.

10. The practice has procedures for security incident reporting and handling. It should have a person or team to take the lead on responding to security incidents.

11. The practice should have procedures for backing up client data. In case something happens to an individual computer or entire server, the practice can

57 One possible division of responsibility is between a lawyer/sponsor with budgetary authority and a staff member with technical expertise and day-to-day responsibility.

recover the data to make sure lawyers and staff members can continue having
access to their emails, texts, and files after their loss.

12. The practice has a disaster recovery and business continuity plan involving
procedures and technology to provide assurances of continued operation in the
event of a natural or man-made disaster. Capabilities for continued resilience of
practice operations are important especially for firms in areas prone to natural
disasters such as hurricanes, floods, tornados, and earthquakes.\(^{59}\)

13. The practice has procedures for assessing the effectiveness of its security
safeguards.

14. The practice supervises third parties, such as service providers and temporary
workers, with access to client data.

15. The practice has certain approved online applications, such as online storage
and file transfer services, and does not permit users to store client data in online
accounts controlled by individual users outside the practice’s control.

16. The practice has cyber risk insurance coverage with appropriate limits of liability
and with appropriate types of coverages.

17. The practice has procedures to minimize the creation of “metadata” (such as
comments and tracked changes) that could reveal attorney-client communication
or other sensitive information to opponents when exchanging word processing
programs, perhaps with the assistance of a metadata scrubbing program.\(^{60}\)

B. Examples of Physical Safeguards

1. The law office has walls, doors, and windows that reasonably prevent physical
intrusion. Any servers are kept in a separate, locked area away from places
where visitors may access.

2. People in waiting areas cannot see the screens of computers in the reception
areas.

3. Workers are trained to prevent the loss or theft of mobile devices or media, e.g.,
while out of the office. For instance, workers are trained not to leave electronic
devices in visible areas of parked cars.

4. The practice maintains an inventory of computing devices used by lawyers and
staff.

5. Paper records are locked and desks are cleared of paper documents when they
are not needed.

482 (2018). “Lawyers must be prepared to deal with disasters.” Id. at 12.

\(^{60}\) See generally ABA Comm. on Ethics and Professional Responsibility, Formal Op. 06-
6. The practice wipes electronic data off of computers, mobile devices, and portable electronic media before they are transferred, sold, or reused. The practice shreds discarded work papers.

C. Examples of Technical Safeguards

1. The practice controls access to systems with client data using strong passwords or other authentication mechanisms.
   a. We believe that small practices should now use (or now start the transition to) more than one “factor” of security access to critical applications, such as webmail.
   b. A “factor” can be something you know (e.g., a password), something you have (e.g., a security hardware device), or something you are (a biometric identifier, such as fingerprint).
   c. In one common scenario, for example, to log into the application, a user would have to input a user name and password (something to user knows) as well as a text message sent to the user’s cell phone. A remote attacker with the password but without access to the user’s cell phone could not log in.
   d. The practice uses strong passwords and/or biometric mechanisms to control access to smart phones.
   e. The practice password protects its wireless networks with strong passwords.

2. Individual workers have their own accounts on the practice’s network and computers.

3. Workstations log off users after a period of inactivity or otherwise require the user to reauthenticate him or herself to the system.

4. The practice encrypts client data while stored on computers, mobile devices, and any servers.

5. The practice promptly patches operating system and application software. When solos and individual users manage their systems, it is usually best to establish settings for automatic software updates. Larger practices may want central management of software updates.

6. The practice has procedures to remotely wipe lost or stolen mobile devices containing client data.

---

61 The use of text messages sent to a cell phone as a second factor of authentication has known weaknesses, but the ubiquity of cell phones makes the use of text messages easy to implement for smaller practices and greatly reduces the risks associated with reliance on passwords alone.
7. When exchanging sensitive information with clients, the practice uses industry-standard methods and software for encryption.62
8. Remote users logging into office computers use remote access software or a virtual private network to encrypt communications between the user’s device and the office computer.
9. Networks and computer systems log user activity. Common operating systems maintain useful system logs by default.
10. The practice uses industry-standard endpoint security software, including firewalls for individual computers and antivirus components to prevent and detect malicious software.
11. The practice’s networks are protected by technologies to control access, such as firewalls. Larger practices should consider implementing specific network protection technologies for intrusion detection, data loss prevention, and continuous monitoring.
12. The guest wireless network should be segregated from the practice’s internal network.
13. Larger practices should consider products and services that filter emails, for example to prevent spam and malicious software, and products and services for filtering web traffic, which can, for instance, prevent access to malicious sites hosting malicious software or block access to certain kinds of sites.

V. Conclusions

All lawyers, including solos and small firms, have ethical duties to maintain the confidentiality of client data used in their practices, to act competently in their practices, and to supervise staff and third parties with access to client data. These duties appear in the ABA Model Rules of Professional Conduct and state rules of professional conduct. These are non-delegable duties. Lawyers must provide leadership and manage the information security functions in their firms and not simply turn over all information security functions to their staffs.

With increasing information security threats from various state and non-state actors, coupled with rapid advances in technology and how it is used, law firms face ever-greater threats to client data. The rules call for attorneys to use reasonable care to

62 ABA Formal Opinion 477 states that lawyers can transmit information relating to a representation over the Internet if they exercise reasonable care to prevent inadvertent or unauthorized disclosure, but where the nature of the information, client agreement, or legal duty requires heightened security, the lawyer may be required to use special security measures for transmission. ABA Comm. on Ethics and Professional Responsibility, Formal Op. 477 (2017).
protect client data. An effective security program of administrative, physical, and technical safeguards can help a law firm and its lawyers mitigate their information security risks and comply with ethical obligations. Solos and small firms can and must implement reasonable safeguards that are appropriate for the size of their practices. Over time, there will be breaches. Nonetheless, if small practices implement and maintain an effective information security program, they can effectively manage their risk of breaches and resulting liability.

For more information, contact:
Stephen Wu, ssw@svlg.com, 408.573.5737
Drew Simshaw, dts52@georgetown.edu, 202.662.9067
An Overview of Cybersecurity Legal Requirements for All Businesses
2019 Update
Thomas J. Smedinghoff

TABLE OF CONTENTS

A. WHAT IS DATA SECURITY? .......................................................................................................... 2

B. THE DUTY TO PROVIDE SECURITY .......................................................................................... 4

1. Where Does the Duty to Provide Security Come From? ............................................................ 4
   (a) Statutes and Regulations .................................................................................................. 4
   (b) Common Law Obligations ............................................................................................... 7
   (c) Rules of Evidence ......................................................................................................... 7
   (d) Contractual Obligations .................................................................................................. 8
   (e) Self-Imposed Obligations ............................................................................................... 8

2. What Is the Nature of the Legal Obligation? .................................................................................. 9

   (a) Identify Information Assets ............................................................................................ 12
   (b) Conduct a Periodic Risk Assessment ............................................................................. 13
   (c) Select and Implement Responsive Security Controls to Manage and Control Risk .... 16
      (1) Relevant Factors to Consider .................................................................................... 17
      (2) Categories of Security Measures that Must Be Addressed ...................................... 18
   (e) Monitoring and Testing ................................................................................................. 20
   (f) Oversee Third Party Service Provider Arrangements .................................................... 20
   (g) Review and Adjustment ................................................................................................. 21

---

1 Thomas J. Smedinghoff is Of Counsel in the Privacy & Cybersecurity Practice Group at the law firm of Locke Lord LLP, in Chicago. He is Co-Chair of the ABA Cybersecurity Legal Task Force, and Chair of the Identity Management Legal Task Force and Co-Chair of the Cybersecurity Subcommittee of the ABA Section of Business Law, Cyberspace Committee. He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law (“UNCITRAL”), where he participated in the negotiation of the United Nations Convention on the Use of Electronic Communications in International Contracts. Mr. Smedinghoff is co-editor and contributing author of the GUIDE TO CYBERSECURITY DUE DILIGENCE IN M&A TRANSACTIONS (American Bar Association, 2017), and a contributing author to the 1st and 2nd editions of: THE ABA CYBERSECURITY HANDBOOK - A RESOURCE FOR ATTORNEYS, LAW FIRMS & BUSINESS PROFESSIONALS (ABA, 2013 and 2018). He is also the author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (2008). He can be reached at Tom.Smedinghoff@lockelord.com.
TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Special Rules for Specific Data Elements</td>
<td>22</td>
</tr>
<tr>
<td>(a) Sensitive Data</td>
<td>22</td>
</tr>
<tr>
<td>(b) Social Security Numbers</td>
<td>22</td>
</tr>
<tr>
<td>(c) Credit Card Data</td>
<td>22</td>
</tr>
<tr>
<td>5. Special Rules for Specific Security Controls</td>
<td>23</td>
</tr>
<tr>
<td>(a) Duty to Encrypt Data</td>
<td>23</td>
</tr>
<tr>
<td>(b) Data Destruction</td>
<td>23</td>
</tr>
<tr>
<td>C. THE DUTY TO WARN OF SECURITY BREACHES</td>
<td>27</td>
</tr>
<tr>
<td>1. The Basic Obligation</td>
<td>27</td>
</tr>
<tr>
<td>2. International Adoption</td>
<td>28</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>29</td>
</tr>
</tbody>
</table>
An Overview of Cybersecurity Legal Requirements for All Businesses

What are the cybersecurity legal obligations generally applicable to all U.S. businesses?

It is well known that certain sectors of the U.S. economy are subject to extensive regulations regarding data security. The most obvious examples are the financial sector, the healthcare sector, the federal government sector, and other critical infrastructure sectors. But what about companies in non-regulated sectors?

There is also no doubt that non-regulated businesses are subject to data security obligations. One need look no further than the numerous FTC and state attorney general enforcement actions since 2002 to see that regulated and non-regulated companies alike have been targeted for failure to provide appropriate data security for their own corporate data. Examples include software vendors (Microsoft and Guidance Software), consumer electronics companies (Genica and Computer Geeks), mobile app developers (Delta Airlines), clothing retailers (Guess! and Life Is Good), music retailers (Tower Records), animal supply retailers (PetCo), general merchandise retail stores (BJ’s Wholesale, TJX companies,)

---

2 For purposes of this paper, the terms cybersecurity, data security, and information security are treated as synonymous.


7 FTC V. Microsoft (Consent Decree, Aug. 7, 2002), available at www.ftc.gov/os/caselist/0123240/0123240.shtm


11 In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), available at www.ftc.gov/os/2003/06/guessagree.htm

12 In the Matter of Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046


and Sears\textsuperscript{17}), shoe stores (DSW),\textsuperscript{18} restaurant and entertainment establishments (Dave & Busters\textsuperscript{19} and Briar Group\textsuperscript{20}), social media sites (Twitter\textsuperscript{21} and Facebook\textsuperscript{22}), bookstores (Barnes & Noble),\textsuperscript{23} property management firms (Maloney Properties, Inc.),\textsuperscript{24} and hotels (Wyndham).\textsuperscript{25}

The thesis of this paper is that all businesses, whether regulated or not, are generally subject to legal duties regarding the security of their corporate data. Those duties can be summarized as: (1) a duty to protect the security of their corporate data, and (2) a duty to disclose security breaches when they occur. The following sections will explain the source and scope of those duties. But first we begin with a general overview of the concept of data security itself.

A. WHAT IS DATA SECURITY?

Security is the protection of assets (such as buildings, equipment, cargo, inventory, and in some cases, people) from threats. Cybersecurity (or data security, or information security) has been generally described as “the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities,”\textsuperscript{26} and as "the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations.”\textsuperscript{27}

The terms data security, information security and cybersecurity are often used interchangeably, although some might argue that each has a somewhat different emphasis. But regardless of the label, the focus is on the protection of both (1) information systems\textsuperscript{28} -- i.e., computer systems, networks, and

\textsuperscript{17} In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm
\textsuperscript{19} In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm
\textsuperscript{23} http://www.steptoe.com/assets/attachments/514.pdf
\textsuperscript{24} See, “Massachusetts Attorney General Announces $15,000 Settlement with Property Management Firm” at http://bit.ly/GU8iNU.
\textsuperscript{28} The Homeland Security Act of 2002 defines the term “information system” to mean “any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes – (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources.” Homeland Security Act of 2002, Pub. L. 107-296, at Section 1001(b), amending 44 U.S.C. § 3532(b)(4).
software, and (2) the *data, messages, and information* that are typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.²

Measures designed to protect the security of information systems and data are generally grouped into three categories, which are typically referred to as follows:

- **Physical security measures**: These are security measures which are designed to protect the tangible items that comprise the physical computer systems and networks that process, communicates, and store the data, including servers, devices used to access the system, storage devices, and the like. Examples include fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors and alarm bells.

- **Technical security measures**: These are security measures which involve the use of safeguards incorporated into computer hardware, software, and related devices. They are designed to ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate. Examples include: firewalls, intrusion detection software, access control software, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.

- **Administrative security measures**: Sometimes referred to as “procedural” or “organizational” security measures, these are security measures which consist of management procedures and constraints, operational procedures, accountability procedures, policies, and supplemental administrative controls to prevent unauthorized access and to provide an acceptable level of protection for computing resources and data. Administrative security procedures frequently include personnel management, employee use policies, training, and discipline.

Within each of these three categories, security measures are further classified as preventative, detective, or reactive. Preventative security measures are designed to prevent the occurrence of events that compromise security. An example of a preventative security measure is a lock on a door (to prevent access to a room containing computer equipment), or a firewall (to prevent unauthorized online access to a computer system). Detective security measures are designed to identify security breaches after they have occurred. An example of a detective security measure is a smoke alarm (which is designed to detect a fire), or intrusion detection software (which is designed to detect and track unauthorized online access to a computer system). Reactive security measures are designed to respond to a security breach, and typically include efforts to stop or contain the breach, identify the party or parties involved, and allow recovery of information that is lost or damaged. An example of reactive security is calling the police after an alarm detects that a burglary is in process, or shutting down a computer system after intrusion detection software determines that an unauthorized user has obtained access to the system.

The objectives to be achieved through the use of security measures can be defined in terms of either the positive results to be achieved or the negative consequences to be avoided. The positive results to be achieved are typically described as (1) ensuring the *availability* of systems and information, (2) controlling *access* to systems and information, and (3) ensuring the *confidentiality, integrity, authenticity* of data, messages, and information.

² The *data, messages, and information* to be protected potentially includes a wide variety of data, such as personally identifiable information about employees, customers, prospects, and other individuals; corporate financial information, information regarding corporate business transactions, trade secrets and other confidential information, information relating to corporate communications, including e-mail, and a variety of other types of corporate data. It can also take a variety of forms, including data, messages, documents, voice recordings, images, video, software, and other content in both electronic and paper form.
of information. The harms to be avoided are often described as unauthorized access, use, disclosure or transfer, modification, alteration, or processing of data, and accidental loss or destruction of data.

Achieving these objectives involves implementing security measures designed to protect systems and information from the various threats they face. What those threats are, where they come from, what is at risk, and how serious the consequences are, will of course, vary greatly from case to case. But responding to the threats a company faces with appropriate physical, technical, and organizational security measures is the focus of the duty to provide security.

B. THE DUTY TO PROVIDE SECURITY

Concerns regarding individual privacy, corporate governance, accountability for financial information, the authenticity and integrity of transaction data, and the confidentiality and security of sensitive business data are driving the enactment of new laws and regulations designed to ensure that businesses adequately address the security of their own data. In addition to sector-specific regulations, legislative and regulatory initiatives are imposing obligations on all businesses to implement information security measures to protect their own data and to disclose breaches of security that do occur.

1. Where Does the Duty to Provide Security Come From?

There is no single law, statute, or regulation that governs a non-regulated company’s obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of generally-applicable state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide “reasonable” or “appropriate” security for corporate data. And these obligations apply to both regulated and non-regulated industries.

When viewed as a group they cover a large segment of corporate activity. The most common sources of obligations to provide data security include the following:

(a) Statutes and Regulations

Numerous statutes and regulations impose obligations on businesses to provide security. Some are sector-specific comprehensive security regulations. Other generally-applicable laws are readily recognized by the fact that they are labeled as security laws or use terms such as “security,” “safeguards,” or “protection.” But in many cases the fact that they impose security obligations is evident only by their inclusion or use of terms relating to the attributes of security, such as “authenticate,” “integrity,” “confidentiality,” “availability of data,” and the like. Some of the most common sources of statutory and regulatory obligations to provide cybersecurity include:

---


31 Many of the foreign privacy laws focus their security requirements from this perspective. This includes, for example, EU GDPR Article 32(2); Albania Act, Article 9; Argentina Act, Article 9(1); Australia Act, Schedule 3, Section 4.1; Canada Act, Schedule 1, Section 4.7.1; Hong Kong Act, Principle 4; Philippines Act, Article 8.1; Russia Act, Section 19(1); Singapore Model Code, Principle 7, Section 4.7.1; United Arab Emirates Act, Articles 15(1) and 16(1).


33 See, e.g., E-SIGN, 15 USC 7001 et seq. and UETA.
(1) **Privacy Laws.** The obligation to provide adequate security for personal data collected, used, and/or maintained by a business is a critical component of almost all privacy laws. Most statements of basic privacy principles include security as a key component, and most privacy laws and regulations typically require companies to implement information security measures to protect certain personal data they maintain about individuals.

In the United States protecting personal information is the focus of numerous federal and state privacy laws and regulations. In addition to sector-specific privacy laws and regulations such as GLB (financial sector), HIPAA (healthcare sector), and the Privacy Act of 1974 (federal government), and numerous federal and state privacy laws that target specific types of data, also include security requirements. This includes the federal Children’s Online Privacy Protection Act (COPPA), which applies to all businesses collecting personal information on the Internet from children, as well as numerous state laws relating to credit card information, personal information, and social security numbers.

(2) **Data Security Laws and Regulations.** Separate from privacy laws, several states have enacted laws imposing a general obligation on all companies to ensure the security of personal information and other corporate data. The first was California, which enacted legislation in 2004 requiring all businesses to “implement and maintain reasonable security procedures and practices” to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure. Several other states have followed suit. These include, most notably, the comprehensive Massachusetts data security regulations, and the New York State Department of Financial Services security regulations. State laws governing secure data destruction also fall in to this category.

Some federal regulations also impose a duty to provide for the security of data and systems. Examples include IRS regulations that require companies to implement information security to protect electronic tax records, and SEC regulations regarding protection of corporate financial data, as well as sector-specific regulations such as GLB and HIPAA.

(3) **E-Transaction Laws.** E-transaction laws require appropriate data security to ensure the enforceability of electronic records and for compliance with electronic recordkeeping requirements. Both

---


35 These include Arkansas, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.


37 See list in Appendix.

38 201 CMR 17.00 et seq., available at [http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf](http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf)

39 New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500.02.

the federal and state electronic transaction statutes (E-SIGN and UETA) require all companies to provide
security for storage of electronic records relating to online transactions. For example, they focus on the
security requirements of data integrity and accessibility, and require that an electronic record must
“accurately reflect the information set forth in the record after it was first generated in its final form,” and
that it must “remain accessible for later reference.”

(4) Corporate Governance Legislation. Corporate governance legislation designed to protect
the company and its shareholders, investors, and business partners, such as Sarbanes-Oxley and
implementing regulations, require public companies to ensure that they have implemented appropriate
information security controls with respect to their financial information. In addition, SEC disclosure
guidance issued on October 13, 2011 and updated on February 21, 2018 identifies cyber risks and
incidents as potential material information to be disclosed under existing securities law disclosure
requirements and accounting standards.

(5) Unfair & Deceptive Business Practice Laws. Unfair business practice laws (such as FTC
Act Section 5, which prohibits “unfair or deceptive acts or practices in or affecting commerce,” and
equivalent state laws) and related government enforcement actions are frequently used as a basis for
regulating security.

Through a series of enforcement actions and consent decrees beginning in 2002, both the FTC and
several state attorneys general have, in effect, extended security obligations regarding personal
information to non-regulated industries by virtue of Section 5 of the FTC Act and similar state laws.
Initially, cases were based on the alleged failure of companies to provide adequate information security
contrary to representations they made to customers. In other words, these were claims of deceptive trade
practices. But beginning in June 2005, the FTC significantly broadened the scope of its enforcement
actions by asserting that a failure to provide appropriate information security for consumer personal
information was itself, an unfair trade practice – even in the absence of any false representations by the
defendant as to the state of its security.

(6) Breach Notification Laws. In addition to the legal obligation to implement security
measures to protect corporate data, many laws impose an obligation to disclose security breaches to the
persons affected. But unlike laws that impose a duty to provide security, these laws typically require that
companies disclose security breaches to those who may be adversely affected by such breaches and
man cases, to the state’s attorney general.

---

41 See e.g., UETA at Section 12. See also E-SIGN at 15 USC Sections 7001(d) and (e).
42 See generally, Bruce H. Nearon, Jon Stanley, Steven W. Teppler, and Joseph Burton, Life after Sarbanes-Oxley: The Merger of
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
44 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746, at
45 15 USC Section 45.
46 See e.g., FTC security enforcement actions, listed at https://www.ftc.gov/enforcement/cases-proceedings/terms/249.
47 The FTC’s authority to proceed in this manner was upheld in FTC v. Wyndham Worldwide Corporation, 2015 U.S. App.
All states in the U.S., plus the District of Columbia, Puerto Rico, and the Virgin Islands, have enacted security breach notification laws, all generally based on a 2003 California law. The U.S. federal banking regulatory agencies also require financial institutions to disclose breaches, and the HITECH Act and associated regulations also require notice in the event of a breach. Internationally, many countries are also increasingly requiring breach notification.

(b) Common Law Obligations

Some case law also recognizes that there may be a common law duty to provide data security, the breach of which constitutes a tort. Most recently, for example, in *Dittman v. UPMC* the Pennsylvania Supreme Court held that “in collecting and storing its employees’ personal data on its computer systems, [the employer] owed its employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act.” Several years earlier, in *Bell v. Michigan Council*, a Michigan court held that “defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information.” Likewise, in the case of *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, the court recognized the existence of a legal duty to provide security, noting as follows:

Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer’s confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. See, e.g., *Witriol v. LexisNexis Grp.*, No. C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006); *CUMIS Ins. Soc’y., Inc. v. BJ’s Wholesale Club, Inc.*, No. 051158, 2005 WL 6075375, at *4 (Mass. Super. Dec. 7, 2005) aff’d, 918 N.E.2d 36 (Mass. 2009); *Yakubowicz v. Paramount Pictures Corp.*, 536 N.E.2d 1067, 1070 (Mass. 1989) (“A basic principle of negligence law is that ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm.”). As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.

(c) Rules of Evidence

Providing appropriate security necessary to ensure the integrity of electronic records (and, where necessary, the identity of the creator, sender, or signer of the record) will likely be critical to the

---


45 CFR Part 164.

See, e.g., the EU GDPR at Articles 33 and 34.


admissibility of the electronic record in evidence in a future dispute. This conclusion is supported both by case law\(^\text{56}\) as well as provisions relating to the form requirement for an “original” in electronic transaction legislation.\(^\text{57}\)

In particular, the Ninth Circuit decision in the case of *American Express v. Vinhnee*\(^\text{58}\) suggests that use of appropriate security may be a condition for the admissibility in evidence of electronic records. The bottom line is that, in many situations, the admissibility of all types of electronic data will depend, on the level of information security provided in order to ensure that the integrity and availability of the information remains intact.

(d) **Contractual Obligations**

Data security obligations are often imposed by contract as well. As businesses increasingly become aware of the need to protect the security of their own data, they frequently try to satisfy their obligation (at least in part) by contract in those situations where third parties will have possession of, or access to, their business data. This is particularly common, for example, in outsourcing and cloud service arrangements where a company’s data will be stored with and/or processed by a third party. In addition, in any situation where a business may have access to data of a trading partner, it is quite common for the trading partner to contractually impose security obligations with respect to that data.

Security obligations are also typically imposed by contract in connection with participation in a multi-party system. For example, merchants desiring to accept credit cards must contractually agree to comply with the requirements of the Payment Card Industry Data Security Standard\(^\text{59}\) as a condition of accepting credit cards. Similarly, businesses that want to originate electronic payment orders (e.g., to debit a customer’s bank account) must agree to the rules of the applicable electronic payment systems (such as the ACH payment system), which rules include data security provisions.

(e) **Self-Imposed Obligations**

In many cases, security obligations are also self-imposed. This commonly occurs, for example, through statements in privacy policies, on websites, or in advertising materials, companies often make representations regarding the level of security they provide for their data (particularly the personal data they collect from the persons to whom the statements are made). See, e.g., *Equifax Ruling Shows How Cyber Boasts Can Bring Legal Pain*, Law360 (January 31, 2019).\(^\text{60}\)

Likewise, when companies voluntarily self-certify under the U.S.-EU Privacy Shield Framework,\(^\text{61}\) they represent that they comply with the seven Privacy Shield Principles.\(^\text{62}\) Those Principles include a security requirement that “Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss,


\(^{\text{57}}\) See, e.g., UETA Section 12, and E-SIGN, 15 USC Section 7001(d).


\(^{\text{59}}\) Available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).


\(^{\text{61}}\) See generally [https://www.privacyshield.gov](https://www.privacyshield.gov).

\(^{\text{62}}\) [https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg](https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg)
misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.”

By making such public statements or representations, companies impose on themselves an obligation to comply with the standard they have represented to the public that they meet. If those statements are not true, or if they are misleading, such statements may become, in effect, deceptive trade practices under Section 5 of the FTC Act, or under equivalent state laws. Through a series of enforcement actions and consent decrees, both the FTC and several state attorneys general have used those deceptive business practice statutes to bring enforcement actions against the offending companies.

2. **What Is the Nature of the Legal Obligation?**

The duty to provide data security is often simply stated in the law as an obligation to implement “reasonable” or “appropriate” security measures designed to achieve the security objectives noted above.

In Europe, for example, the GDPR requires organizations to “implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”

In the United States, state security laws, such as in California, generally require “reasonable security procedures and practices.” Federal laws and regulations do the same. For example, HIPAA requires “reasonable and appropriate” security, and the GLB security regulations require security appropriate to the size and complexity of the bank and the nature and scope of its activities.

In other words, the law views security as a relative concept, and recognizes that what qualifies as reasonable security varies with the situation. Thus, the law typically provides little or no guidance on what specific security measures are required, or on how much security a business should implement to satisfy those legal obligations. Most laws do not include any specific requirements regarding whether or not a particular security measure must be implemented, and there are generally no safe harbors. In light of such standards, the choice of security measures and technology can vary depending on the situation.


Laws requiring that companies implement “reasonable” or “appropriate” security often provide little or no guidance as to what is required for legal compliance. Legal developments over the past few years, however, suggest that a legal standard for “reasonable” security is clearly emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like), and instead adopts a fact-specific approach to corporate security obligations that requires a “process” applied to the unique

---

63 Privacy Shield Principle No. 4.
64 GDPR Article 32(1) (emphasis added). See also UK – Data Protection Act 1998, Schedule 1, Part I, Seventh Principle.
65 Cal. Civil Code § 1798.81.5(b).
68 There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.
69 But see Ohio Data Protection Act, ORC 1354, discussed below.
facts of each case. It puts the focus on identifying and responding to the particular threats a business faces.

Rather than telling companies what specific security measures they must implement, the emerging legal standard requires companies to engage in an ongoing and repetitive process that is designed to identify and assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. The decision regarding the specific security measures is left up to the company.

This approach recognizes that there are a variety of different security measures responsive to specific threats, and recognizes that threats (and appropriate responsive security measures) are constantly changing. Thus, the presence or absence of specific security measures says little about the status of a company’s legal compliance with its information security obligations. Because armed guards at a the front of a building do not protect against hackers accessing information through the Internet, and because firewalls designed to stop hackers do not protect against dishonest employees with authorized access, the law puts its focus on implementing those security measures that respond to the specific threats a business faces.

At its essence implementing “reasonable” or “appropriate” security compliance requires a company to develop and implement a risk-based “security program” based on a process-oriented approach whereby it does the following:

- **Assign Responsibility:** Designate one or more employees to be responsible for the security program;
- **Identify Information Assets:** Identify the corporate information assets that need to be protected, including (1) data records containing personal information or other sensitive confidential information, and (2) information systems used to process, store, and communicate the relevant data, such as computing systems, networks, and storage media (including laptops and portable devices);
- **Conduct Risk Assessment:** Periodically conduct a risk assessment to identify and assess internal and external risks to the security, confidentiality, and/or integrity of its information assets, and evaluate the effectiveness of the safeguards currently in place for minimizing such risks;
- **Select and Implement Responsive Security Controls:** Select and implement appropriate physical, administrative, and technical security controls to minimize the risks identified in the risk assessment;
- **Monitor Effectiveness:** Regularly monitor and test the security controls that have been implemented to ensure that the security program is operating in a manner reasonably calculated to protect the information assets; and upgrade the security controls as necessary to limit risks;
- **Regularly Review Program:** Review and adjust the security program on a regular basis, including: (i) whenever there is a material change in business practices that could affect the security of the information, and (ii) following any incident involving a breach of security; and
- **Address Third Party Issues:** Take all reasonable steps to (1) verify that each third-party service provider that has access to the information assets has the capacity to protect such information assets in the manner required by the risk assessment; (2) obligate such party by contract to actually implement such security, and (3) take reasonable steps to ensure that each third party service provider is actually applying such security measures as required by the contract.
A key aspect of this process is recognition that it is never completed. It is ongoing, and must be continually reviewed, revised, and updated.

This “risk-based” legal standard for corporate information security has come to be known as a requirement to develop, implement, and maintain a “comprehensive information security program” (WISP), or simply a “security program.”

The legal requirement for such a risk-based security program was first set forth in a series of financial industry security regulations required under the Gramm-Leach-Bliley Act (GLBA) titled Guidelines Establishing Standards for Safeguarding Consumer Information. They were issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001, and later adopted by the FTC in its GLBA Safeguards Rule on May 23, 2002. The same approach was also incorporated in the Federal Information Security Management Act of 2002 (“FISMA”), and in the HIPAA Security Standards issued by the Department of Health and Human Services on February 20, 2003.

Shortly thereafter, the FTC also adopted the view that the risk-based process-oriented approach to information security outlined in these regulations sets forth a general “best practice” for legal compliance that should apply to all businesses in all industries. Thus, the FTC has, in effect, implemented this process oriented requirement for a risk-based security program in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security. The National Association of Insurance Commissioners has also recommended the same approach in its Insurance Data Security Model Law.

In 2010 this approach was formally adopted by Massachusetts in its data security regulations, which require businesses to develop a comprehensive written information security program, and set out detailed

---


73 44 U.S.C. Section 3544(b).

74 45 C.F.R. Parts 164.


76 See, e.g., FTC Decisions and Consent Decrees listed at https://www.ftc.gov/enforcement/cases-proceedings/terms/249.


78 201 CMR 17.00 et. seq.
requirements for such a security program. Likewise, the 2017 New York DFS Regulations adopt the same approach. In the EU, a similar requirement is referenced in GDPR.

The importance of a written security program is also being recognized in recent statutory updates. A change to the Massachusetts breach notification statute, for example, requires companies to notify the Attorney General in the event of a data breach, and as part of that notification, to indicate whether they maintain a written information security program.

In sum, the law recognizes what security consultants have been saying for some time: “security is a process, not a product.” Legal compliance with security obligations involves a risk-based process applied to the facts of each case in order to achieve an objective (i.e., to identify and implement the security measures appropriate for that situation), rather than the implementation of standard specific security measures in all cases. Thus, there will likely be no hard and fast rules. Instead, the legal obligation regarding security focuses on what is reasonable under the circumstances to achieve the desired security objectives.

Based on existing law and regulations, the required steps for developing a comprehensive information security program as the means of achieving reasonable security may be summarized as follows:

(a) **Identify Information Assets**

In order to protect something, you need to know what it is, where it is, how it is used, how valuable it is, and so forth. Thus, when addressing data security, the first step is to identify the information assets to be protected so as to define the scope of the effort.

This involves taking an inventory of the data and information that that organization creates, collects, receives, uses, processes, stores, and communicates to others. It also requires examining the systems, networks and processes by which such data is created, collected, received, used, processed, stored, and communicated.

Understanding where the data and systems are located is also important. This requires identifying where in the organization (e.g., which office and which department), the data and systems are located, and who controls them. It also requires identifying in which jurisdictions (country and state or province) they are collected, processed, and stored, as this will impact which laws must be complied with.

Moreover, it is also important to consider the organization’s data that is in the possession and control of a third party, such as an outsource service provider or cloud provider, as the organization is responsible for the security of all of its data regardless of who has actual possession of it.

---

28 201 CMR 17.00 et. seq.

29 N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.02 and 500.03.

30 GDPR. Article 32.

31 Mass. Gen. Laws. Ch. 93H, Section 3(b) (effective April 11, 2019)

(b) **Conduct a Periodic Risk Assessment**

Implementing a comprehensive security program to protect these information assets requires a thorough assessment of the potential risks to the organization’s information systems and data.

A *risk assessment* is the process of identifying, estimating, and prioritizing information security risks to the business. The purpose of a risk assessment is to inform decision makers and support the development and implementation of "appropriate" and "reasonable" security controls to respond to the risks identified.

*Risk* is a measure of the extent to which the business is threatened by a potential circumstance or event. It is typically a function of: (i) the likelihood of the occurrence of an adverse event or threat, and (ii) the adverse impacts that would result if such an adverse event or threat does materialize. Thus, assessing risk requires: (i) identifying relevant *threats* to the business; (ii) identifying *vulnerabilities* both internal and external to the business; (iii) assessing the *likelihood* that such threats will occur and exploit the vulnerabilities to cause harm, and (iv) evaluating the *impact* (i.e., harm) to the business that may result if the threat does occur and is able to exploit the vulnerabilities. The end result is a determination of risk.

- **A threat** is anything that has the potential to cause harm to the information assets. Examples of threats include: (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization, such as a fire, flood, or tornado; or (v) technical and personal threats such as from malware, a computer virus, the actions of a hacker, or the negligent mistake of an employee.

- **A vulnerability** is a flaw or weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source—i.e., that can be accidentally triggered or intentionally exploited by the threat to endanger or cause harm to an information asset. It might be a hole in the roof, a system with easy to guess passwords, unencrypted data on a laptop computer, disgruntled employees, or employees that simply do not understand what steps they need to take to protect the security of company data.
  - Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness;
  - Some vulnerabilities can arise "over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge. In the context of such change, existing security controls may become inadequate and may need to be reassessed for effectiveness;"
  - Vulnerabilities can also be found in organizational governance structures (e.g., the lack of effective risk management strategies and adequate risk framing, poor intra-agency communications, inconsistent decisions about relative priorities of missions/business functions, or misalignment of enterprise architecture to support mission/business activities);
  - Vulnerabilities can also be found in external relationships (e.g., dependencies on particular energy sources, supply chains, information technologies, and telecommunications providers), mission/business processes (e.g., poorly defined processes or processes that are not risk-
aware), and enterprise/information security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems).

- The **likelihood** that a threat will exploit a vulnerability to cause harm creates a **risk**. Stated differently, where a threat intersects with a vulnerability, risk is present. For example, if the threat is rain, and the vulnerability is a hole in the roof, risk is the likelihood that it will rain, causing water to enter the building through the hole in the roof, and doing damage to the building and/or its contents. Similarly, if the threat is a hacker, and the vulnerability is open Internet access to a server containing sensitive data, risk is the likelihood that a hacker will enter the system and view, copy, alter, or destroy the sensitive data.

- The level of **impact** from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

In other words, **risk** is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

**Risk assessment**, then, requires a process of identifying vulnerabilities and threats to the information assets used by the company, and assessing the potential impact/harm that would result if a threat materializes. This forms the basis on which the company determines what countermeasures (i.e., security controls), if any, it should implement to reduce risk to an acceptable level. Thus, a risk assessment requires:

- Conducting a threat assessment to identify all reasonably foreseeable internal and external threats to the information and system assets to be protected;
- Conducting a vulnerability assessment to identify the company's vulnerabilities that could be exploited by threat sources;
- Assessing the likelihood that each of the threats will materialize, and if so, the probability that it will exploit one or more of the vulnerabilities to cause harm — i.e., identifying the likelihood that threat sources with the potential to exploit weaknesses or vulnerabilities in the system will actually do so;
- Evaluating the potential damage that will result in such case; and
- Assessing the sufficiency of the security controls in place to guard against the threat.

This risk assessment process will be the baseline against which security controls can be selected, implemented, measured, and validated. The goal is to understand the risks the business faces, and determine what level of risk is acceptable, in order to identify appropriate and cost-effective safeguards to combat that risk.

---


86 See, e.g., GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(1); Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02 (b)(1).

87 See, e.g., FISMA, 44 U.S.C. Sections 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(2); Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.09; see also NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012) at p. 29.
Numerous security laws and regulations expressly require a risk assessment as part of a comprehensive security program. And laws and regulations that do not expressly include such a requirement typically do so impliedly.

In the U.S., a risk assessment is expressly required by a variety of security statutes and regulations, such as GLB and HIPAA at the federal level, and the Massachusetts and New York security regulations at the state level. And it is impliedly required by most other security statutes and regulations when they impose an obligation to provide "reasonable" security. Likewise, the consent decrees entered in all FTC enforcement actions have expressly extended the banking and healthcare sector-specific requirements for a risk assessment to all industries generally.

In addition, several U.S. courts have held that a risk assessment plays a key role in determining whether a duty will be imposed and liability found. In Wolfe v. MBNA America Bank, for example, a federal court held that where injury resulting from negligent issuance of a credit card (to someone who applied using the plaintiff’s identity) is foreseeable and preventable, “the defendant has a duty to verify the authenticity and accuracy of a credit account application.” In Bell v. Michigan Council, the court held that where a harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm. On the other hand, in Guin v. Brazos Education, the court held that where a proper risk assessment was done, but a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.

In the EU and other countries, a risk assessment is frequently a required element of the obligation to provide appropriate data security. Many data protection laws expressly require a risk assessment, including the recently implemented EU-wide General Data Protection Regulation (GDPR). Many other laws, however, impliedly require a risk assessment, typically by requiring that the company must provide a level of security "appropriate to the risk."

In most cases, however, the law does not generally specify how to do a risk assessment. In the U.S. the banking regulators have referred financial institutions seeking general information on risk assessments to: (1) the "Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards," and (2) the "FFIEC IT Examination Handbook, Information Security Booklet." The FTC data security cases and enforcement actions are available at www.ftc.gov/datasecurity.

---

90 Mass. Regulations, 201 CMR 17.03(2)(b)
91 N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.09(a)
92 The FTC data security cases and enforcement actions are available at www.ftc.gov/datasecurity.
95 Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 at *13 (D. Minn. Feb. 7, 2006) (finding that where a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).
96 See GDPR, at Recital 83 and Article 32.
General information on conducting a risk assessment is also available in the National Institute of Standards and Technology (NIST) special publication 800-30, Rev. 1 “Guide for Conducting Risk Assessments.”

Massachusetts also provides guidance in its “Small Business Guide: Formulating a Comprehensive Written Information Security Program.”

**(c) Select and Implement Responsive Security Controls to Manage and Control Risk**

Key to providing reasonable security is implementing security measures that are responsive to the specific risks that a company faces. In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Thus, the next step in the process of developing a comprehensive information security program is to select and implement appropriate physical, technical, and administrative security controls to manage and control the risks the company faces, as identified in the risk assessment.

The key to providing legally-compliant security is that the specific security controls selected and implemented must be responsive to the company's fact-specific risk assessment. In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Those security controls must be responsive to the particular threats a business faces, and must address its vulnerabilities.

Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat the company faces is unauthorized remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers and protect sensitive databases, but if a company's major vulnerability is careless (or malicious) employees who succumb to phishing attacks or inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated technical security measures, while important, will not adequately address the insider risk.

The role of the risk assessment in selecting security controls was also stressed by the U.S. banking regulators in their response to questions relating to its regulations for strong authentication. When asked whether a financial institution could forgo a risk assessment and move immediately to implement additional strong authentication controls, the regulators responded with an emphatic "no." As they pointed out, the security requirements for authentication are risk-based, and thus, a risk assessment that

---


102 See, e.g., U.S., GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(B); FISMA, 44 U.S.C. Section 3544(b); Mass. Regulations 201 CMR 17.03(1); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); EU General Data Protection Regulation, at Recital 83 and Article 32.

103 See, e.g., Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.02(b) and 500.03; EU General Data Protection Regulation, at Recital 83 and Article 32.
sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed before implementing any particular controls.¹⁰⁴

When selecting responsive security controls to implement, there are a number of factors that the organization should take into account, as well as categories of security controls identified in the applicable security laws (and any additional categories that are suggested by the risk assessment), that should be considered to reduce the company's risks and vulnerabilities to a reasonable and appropriate level.¹⁰⁵

(1) Relevant Factors to Consider

In determining what security measures should be implemented within a particular organization, existing precedent recognizes that there is no “one size fits all” approach. Which security measures are appropriate for a particular organization will vary, depending upon a variety of factors.

Traditional negligence law suggests that the relevant factors are (1) the probability of the identified harm occurring (i.e., the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.¹⁰⁶ In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that case and on the extent of foreseeable danger.¹⁰⁷ Security regulations take a similar approach, and indicate that the following factors are relevant in determining what security measures should be implemented in a given case:

The following factors are most often cited in security statutes and regulations as relevant to determining what security controls should be implemented to address identified risks in a given case:

- The company's size, complexity, and capabilities
- The nature and scope of the business activities
- The nature and sensitivity of the information to be protected
- The company's technical infrastructure, hardware, and software security capabilities
- The state of the art and technology and security
- The costs of the security measures¹⁰⁸

Interestingly, cost was the one factor mentioned most often, and certainly implies recognition that companies are not required to do everything theoretically possible.

The bottom line is that the legal appropriateness of any particular security control is not determined in the abstract. Instead, it must be determined on the basis of a risk assessment specific to the company and its business, in light of the factors identified above.


¹⁰⁵ See, e.g., HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(B); N.Y. Dep’t of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); EU General Data Protection Regulation, at Recital 83 and Article 32.

¹⁰⁶ See, e.g., United States v. Carroll Towing, 159 F.2d 169, 173 (2d Cir. 1947).

¹⁰⁷ See, e.g., DCR Inc. v. Peak Alarm Co., 663 P.2d 433, 435 (Utah 1983); see also Glatt v. Feist, 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).

¹⁰⁸ See, e.g., U.S., HIPAA Security Regulations, 45 C.F.R. Section 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A and Part II.C (OCC); 16 CFR §314.3(a) (FTC); FISMA, 44 U.S.C. Sections 3544(a)(2) and 3544(b)(2)(B); Mass. Regulations 201 CMR 17.03(1); EU General Data Protection Regulation, at Recital 83 and Article 32.
(2) Categories of Security Measures that Must Be Addressed

Specifying a process still leaves many businesses wondering, “What specific security measures should I implement?” In other words, in developing a security program, what security measures or safeguards should be included?

Generally, the law does not require companies to implement specific security measures or use a particular technology. As expressly stated in the HIPAA security regulations, for example, companies “may use any security measures” reasonably designed to achieve the objectives specified in the regulations.¹⁰⁹ This focus on flexibility means that, like the obligation to use “reasonable care” under tort law, determining compliance may ultimately become more difficult, as there are unlikely to be any safe-harbors for security.

Nonetheless, many security statutes and regulations require that companies consider certain categories of security measures, even if the way in which each category is addressed is not specified. At a high level, most security laws and regulations, for example, require that businesses implement appropriate physical, technical, and administrative (or organizational) security controls.¹¹⁰ Within each of these three very broad categories of security controls, there are many subcategories to consider. NIST Special Publication 800-53 provides a catalog of security and privacy controls to protect organizational operations and assets.¹¹¹

Some laws and regulations go a step further, and identify certain more granular categories of security controls that businesses should consider, in light of the results of their risk assessments and the other factors noted above, such as access controls, training and education, or incident response planning.¹¹²

¹⁰⁹ HIPAA Security Regulations, 45 CFR Section 164.306(b)(1). There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.00.

¹¹⁰ See, e.g., GLB Security Regulations, 12 CFR Part 364, Appendix B, II.A (FDIC); and 16 CFR §314.3(a) (FTC); HIPAA Security regulations, 45 CFR Section 164.308 (Administrative safeguards); 45 CFR Section 164.310 (Physical safeguard), and 45 CFR Section 164.312 (Technical safeguards); Mass. Regulations, 201 CMR 17.03(1); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.03(j); EU General Data Protection Regulation, Articles 5(f) and 32(1).

¹¹¹ NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Updated August 2017), https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf. While this is written to “establish security controls for federal information systems and organizations,” it also notes that “Private sector organizations are encouraged to consider using these guidelines, as appropriate.”

¹¹² Requirement for Access Controls See, e.g., 12 CFR Part 364 (FDIC), Appendix B, III.C.1.a; Security Regulations, 12 CFR Part 364 (FDIC), Appendix B, III.C.2; HIPAA Security Regulations, 45 CFR 164.308(a)(4) (administrative access controls), 164.310(a) (physical access controls), 164.310(a) (technical access controls); Mass. Regulations 201 CMR 17.03(2)(g), 17.04(1)(d), 17.04(2); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.03, 500.07;


Requirement for Incident Response Planning: See, e.g., GLB Security regulations (FTC), 12 CFR Part 364, Appendix B, III.C.1(g); Mass. Regulations, 201 CMR 17.03(2)(j); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.03(e), 500.03(n), and 500.16; EU General Data Protection Regulation, Article 32(1)(c).
example, many laws require companies to implement access control measures to ensure that only authorized persons can access sensitive data. But the laws typically say nothing about which access controls should be used. At most, they will sometimes define objectives or criteria that must be achieved (such as restricting access on a need to know basis, or requiring that access be terminated when an employee leaves the company). Thus (in the example of access controls), companies are free to select any types of access controls that achieve those objectives and are reasonable for the business in light of the results of its risk assessment. But the key is to consider which security controls within a designated category are appropriate for the company in light of its particular risk assessment.

The general categories of security measures mentioned most often in the various laws, regulations, and security standards include the following:

- **Physical Facility and Device Security Controls** – Procedures to safeguard the facility, measures to protect against destruction, loss, or damage of information due to potential environmental hazards (such as fire and water damage or technological failures), procedures that govern the receipt and removal of hardware and electronic media into and out of a facility, and procedures that govern the use and security of physical workstations.

- **Physical Access Controls** – Access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.

- **Technical Access Controls** – Policies and procedures to ensure that authorized persons who need access to the system have appropriate access, and that those who should not have access are prevented from obtaining access, including procedures to determine access authorization, procedures for granting and controlling access, authentication procedures to verify that a person or entity seeking access is the one claimed, and procedures for terminating access.

- **Intrusion Detection Procedures** – Procedures to monitor log-in attempts and report discrepancies; system monitoring and intrusion detection systems and procedures to detect actual and attempted attacks on or intrusions into company information systems; and procedures for preventing, detecting, and reporting malicious software (e.g., virus software, Trojan horses, etc.).

- **Employee Procedures** – Job control procedures, segregation of duties, and background checks for employees with responsibility for or access to information to be protected, and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means.

- **System Modification Procedures** – Procedures designed to ensure that system modifications are consistent with the company’s security program.

- **Data Integrity, Confidentiality, and Storage** – Procedures to protect information from unauthorized access, alteration, disclosure, or destruction during storage or transmission, including storage of data in a format that cannot be meaningfully interpreted if opened as a flat, plain-text file, or in a location that is inaccessible to unauthorized persons and/or protected by a firewall.

- **Data Destruction and Hardware and Media Disposal** – Procedures regarding final disposition of information and/or hardware on which it resides, and procedures for removal from media before re-use of the media.

- **Audit Controls** – Maintenance of records to document repairs and modifications to the physical components of the facility related to security (e.g., walls, doors, locks, etc); and hardware, software, and/or procedural audit control mechanisms that record and examine activity in the systems.
• **Contingency Plan** – Procedures designed to ensure the ability to continue operations in the event of an emergency, such as a data backup plan, disaster recovery plan, and emergency mode operation plan;

• **Incident Response Plan** – A plan for taking responsive actions in the event the company suspects or detects that a security breach has occurred, including ensuring that appropriate persons within the organization are promptly notified of security breaches, and that prompt action is taken both in terms of responding to the breach (e.g., to stop further information compromised and to work with law enforcement), and in terms of notifying appropriate persons who may be potentially injured by the breach.

• **Awareness, Training and Education** – Training and education for employees to ensure that they understand their roles and responsibilities with respect to security, including communication to employees of applicable security policies, procedures, standards, and guidelines, implementing a security awareness program, periodic security reminders, and developing and maintaining relevant employee training materials, such as user education concerning virus protection, password management, and how to report discrepancies.

(d) **Monitoring and Testing**

Merely implementing security measures is not sufficient. Companies must also ensure that the security measures have been properly put in place and are effective. This includes conducting an assessment of the sufficiency of the security measures in place to control the identified risks, and conducting regular testing or monitoring of the effectiveness of those measures. Existing precedent also suggests that companies must monitor compliance with its security program. To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports is also important.

(e) **Oversee Third Party Service Provider Arrangements**

In today's business environment it is also important to recognize that companies often rely on third parties, such as outsource providers and cloud providers, to handle much of their data. When corporate data is in the possession and under the control of a third party, this presents special challenges for ensuring security.

A company's responsibility for the security of its data includes not only the data in its possession and control, but also its data residing with such third parties. Regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Accordingly, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.

---

113 See, e.g., the FTC data security cases and enforcement actions available at www.ftc.gov/datasecurity.

114 See, e.g., GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III(c)(3); Mass. Regulations 201 CMR 17.03(h); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.05; EU General Data Protection Regulation, at Article 32(1)(d); and the FTC data security cases and enforcement actions available at www.ftc.gov/datasecurity.

115 See, e.g., the FTC data security cases and enforcement actions available at www.ftc.gov/datasecurity.


Thus, any comprehensive information security program must address the security of a company's data held by third parties. Laws and regulations imposing information security obligations on businesses often expressly address requirements with respect to the use of third party outsource providers. First and foremost, they make clear that regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, “you can outsource the work, but not the responsibility.” Thus, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.

Accordingly, security laws and regulations typically impose three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers, (2) they must contractually require outsource providers to implement appropriate security measures, and (3) they must monitor the performance of the outsource providers.

(f) Review and Adjustment

Perhaps most significantly, the legal standard for information security recognizes that security is a moving target. Businesses must constantly keep up with every changing threats, risks, vulnerabilities, and security measures available to respond to them. It is a never-ending process. As a consequence, businesses must conduct periodic internal reviews to evaluate and adjust the information security program in light of:

- The results of the testing and monitoring
- Any material changes to the business or arrangements
- Any changes in technology
- Any changes in internal or external threats
- Any environmental or operational changes
- Any other circumstances that may have a material impact.

In addition to periodic internal reviews, best practices and the developing legal standard may require that businesses obtain a periodic review and assessment (audit) by qualified independent third-party professionals using procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements, and is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, and integrity of information is

---

118 See, e.g., U.S., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(f); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11; EU General Data Protection Regulation, at Articles 28 and 32.

119 See, e.g., Massachusetts Security Regulations, 201 CMR 17.02(2)(f).

120 See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(1); Mass. Regulations 201 CMR 17.03(2)(f)(1); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11.

121 See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(2)(f)(2); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23. § 500.11.

122 See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(3); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11.
protected. It should then adjust the security program in light of the findings or recommendations that come from such reviews.

4. **Special Rules for Specific Data Elements**

In addition to laws imposing general security obligations with respect to personal information, developing law is also imposing new obligations to protect specific data elements or sub-categories of personal data. That is, laws, regulations, and standards are beginning to focus on specific data elements, and imposing specific obligations with respect to such data elements. Prime examples include Social Security numbers, credit card transaction data, and other sensitive data.

(a) **Sensitive Data**

In the EU, the GDPR requires special treatment for particularly sensitive personal information – defined as “special categories” of personal data. Those special categories are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.\(^{123}\) Processing such sensitive data, according to EU interpretation, requires that “special attention” be given to data security aspects to avoid risks of unauthorized disclosure. In particular, “[a]ccess by unauthorized persons must be virtually impossible and prevented.”\(^{124}\)

In the United States, a de facto category of sensitive information has been defined by the various state security breach notification laws. As discussed below, these laws require special action (i.e., disclosure) in the event of a breach of security with respect to a subcategory of personal data generally considered to be sensitive because of its potential role in facilitating identity theft.

(b) **Social Security Numbers**

The security of Social Security numbers has been the particular focus of numerous state laws enacted in recent years (see list in Appendix). The scope of these laws ranges from restrictions on the manner in which Social Security numbers can be used to requirements for security when communicating and/or storing such numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted.\(^{125}\)

(c) **Credit Card Data**

For businesses that accept credit card transactions, the Payment Card Industry Data Security Standards (“PCI Standards”)\(^{126}\) impose significant security obligations with respect to credit card data captured as part of any credit card transaction. The PCI Standards, jointly created by the major credit card associations, require businesses that accept MasterCard, Visa, American Express, Discover, and

\(^{123}\) GDPR, Article 9.


\(^{126}\) Available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).
Diner’s Club cards to comply. At least three states have now incorporated at least part of the PCI Standards in their law.¹²⁷

5. **Special Rules for Specific Security Controls**

(a) **Duty to Encrypt Data**

Some laws and regulations impose obligations to use encryption in certain situations. Initially this included state laws that mandate encryption of Social Security numbers for communication over the Internet.¹²⁸ More recently, however, some state laws prohibit the electronic transmission of any personal information to a person outside of the secure system of the business (other than a facsimile) unless the information is encrypted.¹²⁹ Most notable are the Massachusetts Regulations, which require businesses to encrypt personal information if it is stored on “laptops or other portable devices,” “will travel across public networks,” or will “be transmitted wirelessly.”¹³⁰

(b) **Data Destruction**

Many laws and regulations impose security requirements with respect to the manner in which data is destroyed. These regulations typically do not require the destruction of data, but seek to regulate the manner of destruction when companies decide to do so.

At the Federal level, both the banking regulators and the SEC have adopted regulations regarding security requirements for the destruction of personal data. Similarly, at the State level, several states have now adopted similar requirements.¹³¹

Such statutes and regulations generally require companies to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. With respect to information in paper form, this typically requires implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot be read or reconstructed. With respect to electronic information, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer personal information so that the information cannot practicably be read or reconstructed.¹³²

¹²² See list in Appendix.
¹²⁸ NRS 597.970
¹²⁹ 201 CMR 17.04(3) and (5).
¹³¹ See list in Appendix.
¹³² See, e.g., 16 CFR Section 682.3.
6. **A Safe Harbor for Reasonable Security?**

A first-of-its-kind data security law, the recently enacted Ohio Data Protection Act[^133|ORC 1354 et. Seq.; https://www.ohioattorneygeneral.gov/Business/CyberOhio/Data-Protection-Act] may signal the beginning of a new trend in the legal approach to corporate cybersecurity obligations. At the same time, it may provide some assistance to businesses struggling to ensure that they have implemented legally required data security.

The Ohio Data Protection Act (effective November 1, 2018) introduces two very important concepts relevant to cybersecurity compliance:

- First, the Act implicitly recognizes that compliance with selected industry norms and best practices provide legally compliant “reasonable security;” and
- Second, for businesses that follow one of the approaches designated in the Act, the Act provides a safe harbor in the form of an affirmative defense to any tort action that is brought against the business alleging that its failure to implement reasonable information security controls resulted in a data breach concerning personal information.

To obtain the benefit of the affirmative defense, a business must “create, maintain, and comply with a written cybersecurity program” that satisfies three requirements:

- It must “contain administrative, technical, and physical safeguards . . . *that reasonably conform to an industry recognized cybersecurity framework* as described in [the Act].”[^134|ORC 1354.02(A) (emphasis added)]

- It must “be designed to do all of the following with respect to the [personal and/or restricted information],” as applicable:
  - (1) Protect the security and confidentiality of the information;
  - (2) Protect against any anticipated threats or hazards to the security or integrity of the information;
  - (3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.[^135|ORC 1354.02(B)] and

- The “scale and scope” of the cybersecurity program must be appropriate based on all of the following factors:
  - The size and complexity of the covered entity;
  - The nature and scope of the activities of the covered entity;
  - The sensitivity of the information to be protected;
  - The cost and availability of tools to improve in formation security and reduce vulnerabilities;
  - The resources available to the covered entity.[^136|ORC 1354.02(C)]


[^134|ORC 1354.02(A) (emphasis added)]

[^135|ORC 1354.02(B)]

[^136|ORC 1354.02(C)]
Businesses that meet these requirements are entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information, or restricted information.\textsuperscript{137}

The “industry-recognized cybersecurity frameworks” that qualify for the safe harbor under the Act (and to which an organization’s cybersecurity program must “reasonably conform”) are the following –

For all businesses:

- NIST Cybersecurity Framework\textsuperscript{138}
- NIST Special Publication 800-171 (“Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”)\textsuperscript{139}
- NIST Special Publications 800-53\textsuperscript{140} (“Security and Privacy Controls for Information Systems and Organizations”) and 800-53A (“Assessing Security and Privacy Controls in Federal Information Systems and Organization”)\textsuperscript{141}
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework\textsuperscript{142}
- Center for Internet Security, Critical Security Controls for Effective Cyber Defense\textsuperscript{143}
- International Organization for Standardization / International Electrotechnical Commission 27000 Family of Information Security Standards - information security management systems ISO-27000 family\textsuperscript{144}

For regulated businesses:

- HIPAA security requirements

\textsuperscript{137} ORC 1354.02(D)


\textsuperscript{139} NIST SP 800-171, Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (December 2016); available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171r1.pdf


\textsuperscript{142} FedRAMP Security Assessment Framework, Ver. 2.4 (November 15, 2017); available at https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

\textsuperscript{143} CIS Controls, available at https://www.cisecurity.org/controls/

\textsuperscript{144} ISO/IEC 27000 Family of Information Security Standards, https://www.itgovernance.co.uk/iso27000-family
GLB security requirements
FISMA
Health Information Technology for Economic and Clinical Health Act
PCI standard

This approach appears to recognize that cybersecurity programs based on any of the foregoing provide “reasonable security,” and that providing “reasonable security” is a defense in the case of a breach.

This Ohio statute is the first cybersecurity law providing an express safe harbor for entities that exercise “reasonable security.” However, it should be noted that a few years ago the California Attorney General released a report setting forth what might be described as a reverse safe harbor — i.e., if you don’t take certain steps, then you will be deemed not to have provided legally compliant reasonable security.

In the “California Data Breach Report 2012 – 2015,” the California Attorney General referenced the requirement under California law that businesses implement “reasonable” security, and noted that the Center for Internet Security’s Critical Security Controls for Effective Cyber Defense (the Controls) are designed to address this challenge. But then the Report went further, stating that failure to implement those Controls constitutes a lack of reasonable security. Specifically, the Report states that:

The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.

It is unclear whether either the safe harbor approach adopted by the Ohio statute or the so-called reverse safe harbor approach promoted by the California Attorney General will gain traction. But as businesses struggle with the issue of defining “reasonable security,” we can probably expect to see more law and regulation along these lines.

---


146 See Cal. Civ. Code § 1798.81.5(b), “A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

147 The CIS Critical Security Controls for Effective Cyber Defense, Version 6, October 15, 2015, available from the Center for Internet Security at www.cisecurity.org. Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.

148 Id, at p. 30.

149 Id. (emphasis added)
C. THE DUTY TO WARN OF SECURITY BREACHES

In addition to the duty to implement security measures to protect data, we are also witnessing a global trend to enact laws and regulations that impose an obligation to disclose security breaches to the persons affected, and in many case to regulators as well.

Designed as a way to help protect persons who might be adversely affected by a security breach of their personal information, these laws impose on companies an obligation similar to the common law “duty to warn” of dangers. Such a duty is often based on the view that a party who has a superior knowledge of a danger of injury or damage to another that is posed by a specific hazard must warn those who lack such knowledge. By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons with a warning that their personal information has been compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.\^150

All states in the U.S. have now enacted security breach notification laws, all generally based on a 2003 California law.\^151 These laws are generally applicable to all businesses that maintain data about residents of the enacting state.

1. The Basic Obligation

Taken as a group, the state and federal security breach notification laws generally require that any business in possession of sensitive personal information about a covered individual must disclose any breach of such information to the person affected. The key requirements, which vary from state-to-state, include the following:

- **Type of information** – The statutes generally apply to unencrypted sensitive personally identified information – e.g., information consisting of first name or initial and last name, plus one of the following: social security number, drivers license or other state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account). In some states this list is longer, and may also include medical information, insurance policy numbers, passwords by themselves, biometric information, professional license or permit numbers, telecommunication access codes, mother’s maiden name, employer ID number, electronic signatures, and descriptions of an individual’s personal characteristics.

- **Definition of breach** – Generally the statutes require notice following the unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of such personal information. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the customer.

- **Who must be notified** – Notice must be given to any residents of the state whose unencrypted personal information was the subject of the breach. If a business maintains computerized personal information that the business does not own or license, the business must notify the owner of the

\^150 See, e.g., Recommended Practices on Notice of Security Breach Involving Personal Information, Office of Privacy Protection, California Department of Consumer Affairs, April, 2006 (hereinafter “California Recommended Practices”), at pp. 5-6 (available at www.privacy.ca.gov/recommendations/secbreach.pdf); Interagency Guidance supra note 4 , at p. 15752.

\^151 See list of statutes in Appendix.
information, rather than the individuals themselves. In addition, many states also require notice to the state Attorney General or other relevant regulator.

- **When notice must be provided** – Generally, persons must be notified in the most expedient time possible and without unreasonable delay, although some states now impose a specific time limits, such as 30 days after learning of the breach. In many states the time for notice may be extended for the following reasons:
  - Legitimate needs of law enforcement, if notification would impede a criminal investigation
  - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system

- **Form of notice** – Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only provided the provisions of E-SIGN\(^\text{152}\) are complied with), or by substitute notice.

- **Substitute notice options** – If the cost of providing individual notice is greater than a certain amount (e.g., $250,000) or if more than a certain number of people would have to be notified (e.g., 500,000), substitute notice may be used, consisting of:
  - E-mail when the e-mail address is available, and
  - Conspicuous posting on the company’s web site, and
  - Publishing notice in all major statewide media.

Several of these issues vary from state to state, however, and some have become controversial. One key issue revolves around the nature of the triggering event. In some states, for example, notification is required whenever there has been an unauthorized access that compromises the security, confidentiality, or integrity of electronic personal data. In other states, however, unauthorized access does not trigger the notification requirement unless there is a reasonable likelihood of harm to the individuals whose personal information is involved\(^\text{153}\) or unless the breach is material\(^\text{154}\)

2. **International Adoption**

Although the breach notification concept began in the United States, it is rapidly spreading internationally. The EU formalized breach notification requirements via GDPR in 2018\(^\text{155}\) as did Canada\(^\text{156}\). Several other countries also impose some sort of duty to notify of security breaches including Chile, India, Mexico, Qatar, Russia, and South Korea.

---

\(^\text{152}\) 15 USC Section 7001 *et. seq.* This generally requires that companies comply with the requisite consumer consent provisions of E-SIGN at 15 USC Section 7001(c).

\(^\text{153}\) Arkansas, Connecticut, Delaware, and Louisiana are examples of states in this category.

\(^\text{154}\) Montana and Nevada are examples of states in this category.

\(^\text{155}\) GDPR Articles 33 and 34.

APPENDIX

Key Information Security Law References

A. Federal Statutes

4. **FCRA/FACTA**: Fair Credit Reporting Act,
10. **Privacy Act of 1974**: 5 U.S.C. Section 552a

B. State Statutes

1. **UETA**: Uniform Electronic Transaction Act, Section 12 (now enacted in 47 states).
2. **Law Imposing Obligations to Provide Security for Personal Information**:

    - **Arkansas**: Ark. Code Ann. § 4-110-104(b)
    - **California**: Cal. Civ. Code § 1798.81.5
    - **Delaware**: Del Code, Title 6, § 12B-100
    - **Florida**: Fla. Stat. § 501.171(2)
    - **Illinois**: 815 ILCS 530/45; (also 740 ILCS 14/1 re Biometric Information Privacy Act)
    - **Louisiana**: La. R.S. 51: 3074
    - **Maryland**: Md. Com. Law Code Ann. § 14-3503
    - **Massachusetts**: Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et. seq.
    - **Nevada**: Nev. Rev. Stat. 603A.210
    - **New Jersey**: N.J.A.C. 13:45F-3 (Pre-Proposed New Rules – 12/15/08)
    - **Oregon**: Or. Rev. Stat. Section 646A.622
Rhode Island  R.I. Stat. 11-49.2-2(2) and (3)
Utah  Utah Code Ann. § 13-44-201

3. **Law Imposing Obligations to Provide Security for Medical Information:**

   California  Confidentiality of Medical Information Act (CMIA) (Civ. Code, § 56 et seq.)

4. **Law Imposing Obligations to Provide Security for Credit Card Information:**

   Minnesota  Minn. Stat. Chapter 325E.64
   Washington  RCWA Chapter 19.255

5. **Law Imposing Duty to Encrypt Personal Information:**

   Arizona  Ariz. Rev. Stat. § 44-1373
   California  Cal. Civil Code Section 1798.85(a)(3) [SSN]
   Maryland  Md. Comm. Code § 14-3302(a)(3) [SSN]
   Massachusetts  Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et seq. [Personal Information on laptops, etc]

6. **Data Disposal / Destruction Laws:**

   Alaska  Ala. Stat. §§ 45.48.500 – 45.48.590
   Arkansas  Ark. Code Ann. § 4-110-104(a)
   California  Cal. Civil Code § 1798.81.
   Florida  Fla. Stat. § 501.171(8)
   Hawaii  Haw. Stat Section § 487R-2
   Illinois  815 ILCS 530/40 (all); 815 ILCS 530/30 (state agencies)
   Indiana  Ind. Code § 24-4-14
   Maryland  Md. Code, § 14-3502; Md. HB 208 & SB 194
   Massachusetts  Mass. Gen. laws. Ch. 93I
   Michigan  MCL § 445.72a
   Montana  Mont. Stat. § 30-14-1703
   New Jersey  N.J. Stat. 56:8-162
   North Carolina  N.C. Gen. Stat § 75-64
   Oregon  2007 S.B. 583, Section 12
   Utah  Utah Code Ann. § 13-42-201
   Vermont  Vt. Stat. Tit. 9 § 2445 et seq.
   Washington  RCWA 19.215.020

7. **Security Breach Notification Laws**

   Alabama  2018 S.B. 318, Act No. 396
Alaska  Alaska Stat. § 45.48.010 et seq.
Arizona  Ariz. Rev. Stat. § 18-545
Arkansas  Ark. Code §§ 4-110-101 et seq.
California  Cal. Civ. Code §§ 1798.29, 1798.82
Colorado  Colo. Rev. Stat. § 6-1-716
Connecticut  Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware  Del. Code tit. 6, § 12B-101 et seq.
Georgia  Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Idaho  Idaho Stat. §§ 28-51-104 to -107
Illinois  815 ILCS §§ 530/1 to 530/25
Indiana  Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.
Iowa  Iowa Code §§ 715C.1, 715C.2
Kansas  Kan. Stat. § 50-7a01 et seq.
Kentucky  KRS § 365.732, KRS §§ 61.931 to 61.934
Maine  Me. Rev. Stat. tit. 10 § 1346 et seq.
Minnesota  Minn. Stat. §§ 325E.61, 325E.64
Mississippi  Miss. Code § 75-24-29
Missouri  Mo. Rev. Stat. § 407.1500
Montana  Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 et seq., 33-19-321
New Jersey  N.J. Stat. § 56:8-161 et seq.
New Mexico  2017 H.B. 15, Chap. 36 (effective 6/16/2017)
North Carolina  N.C. Gen. Stat §§ 75-61, 75-65
North Dakota  N.D. Cent. Code §§ 51-30-01 et seq.
Ohio  Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma  Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon  Oregon Rev. Stat. §§ 646A.600 to .628
Rhode Island  R.I. Gen. Laws §§ 11-49.3-1 et seq.
South Carolina  S.C. Code § 39-1-90
Tennessee  Tenn. Code §§ 47-18-2107; 8-4-119
Utah  Utah Code §§ 13-44-101 et seq.
Vermont  Vt. Stat. tit. 9 §§ 2430, 2435
Virginia  Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington  Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia  W.V. Code §§ 46A-2A-101 et seq.
Wisconsin  Wis. Stat. § 134.98
District of Columbia  D.C. Code §§ 28-3851 et seq.
### 8. State SSN Laws

<table>
<thead>
<tr>
<th>State</th>
<th>Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>Ala. Stat. §§ 45.48.400 – 45.48.480</td>
</tr>
<tr>
<td>Arizona</td>
<td>Ariz. Rev. Stat. § 44-1373</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Ark. Code Ann. § 4-86-107; § 6-18-208</td>
</tr>
<tr>
<td>Delaware</td>
<td>Del. Code Ann., tit. 7 § 503</td>
</tr>
<tr>
<td>Florida</td>
<td>Fla. Stat. ch. 97.0585</td>
</tr>
<tr>
<td>Guam</td>
<td>5 GCA §§ 32704; 5 GCA § 32705</td>
</tr>
<tr>
<td>Illinois</td>
<td>815 Ill. Comp. Stat. 505/2QQ; § 815 ILCS 505/2RR</td>
</tr>
<tr>
<td>Kansas</td>
<td>K.S.A. § 75-3520</td>
</tr>
<tr>
<td>Maine</td>
<td>10 M.R.S. § 1272-B</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>Mass. Gen. Laws Ch. 167B, § 14 &amp; § 22</td>
</tr>
<tr>
<td>Minnesota</td>
<td>Minn. Stat. § 325E.59</td>
</tr>
<tr>
<td>Mississippi</td>
<td>Miss. Code Ann. § 25-1-111</td>
</tr>
<tr>
<td>Missouri</td>
<td>Mo. Rev. Stat. § 407.1355</td>
</tr>
<tr>
<td>Montana</td>
<td>Mont. Code Ann. §§ 32-6-306; Mont. Code §§ 30-14-1702, § 30-14-1703</td>
</tr>
<tr>
<td>New Mexico</td>
<td>N.M. Stat. Ann. §§ 57-12B-1 et seq.</td>
</tr>
<tr>
<td>North Dakota</td>
<td>N.D. Cent. Code § 39-06-14</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>Okla. Stat. tit. 40, § 173.1</td>
</tr>
<tr>
<td>Oregon</td>
<td>Or. Rev. Stat. § 107.840</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>R.I. Gen. Laws §§ 6-13-17 and § 6-13-19</td>
</tr>
<tr>
<td>South Dakota</td>
<td>S.D. Codified Laws §§ 32-12-17.10; S.D. Codified Laws §§ 32-12-17.13</td>
</tr>
<tr>
<td>Utah</td>
<td>Utah Code Ann. §§ 31A-21-110</td>
</tr>
<tr>
<td>State</td>
<td>Laws</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vermont</td>
<td>9 V.S.A. § 2440; 2030</td>
</tr>
<tr>
<td>Washington</td>
<td>Rev. Code Wash. (ARCW) § 19.146.205</td>
</tr>
<tr>
<td>West Virginia</td>
<td>W. Va. Code § 17E-1-11</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>Wis. Stat. § 36.32</td>
</tr>
</tbody>
</table>

9. **State SSN Laws Requiring SSN Policies**

<table>
<thead>
<tr>
<th>State</th>
<th>Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecticut</td>
<td>H.B 5658</td>
</tr>
<tr>
<td>Michigan</td>
<td>Mich. Comp. Laws Section 445.84</td>
</tr>
<tr>
<td>New Mexico</td>
<td>N.M. Stat. Sections 57-12B-2-57-12B-3</td>
</tr>
<tr>
<td>New York</td>
<td>NY Gen. Bus. Law Section 3990dd(4)</td>
</tr>
<tr>
<td>Texas</td>
<td>Texas Bus. &amp; Com. Code Sections 35.581 (effective through March 31, 2009)</td>
</tr>
</tbody>
</table>

**C. Federal Regulations**

1. **Regulations Imposing Obligation to Provide Security**
   
   (a) **COPPA Regulations**: 16 C.F.R. 312.8.
   
   (b) **DHS Regulations**: Electronic Signature and Storage of Form I-9, Employment Eligibility Verification, 8 C.F.R. Part 274a(2) (e), (f), (g), and (h) (requiring an effective records security program).
   
   
   (d) **FDA Regulations**: 21 C.F.R. Part 11.
   
   
   
   (g) **GLB Security Regulations (FTC)**: FTC Safeguards Rule (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).
   
   (h) **HIPAA Security Regulations**: Final HIPAA Security Regulations, 45 C.F.R. Part 164.
   
   (i) **HIPAA Breach Notification Rules**: 45 CFR Sections 164.400 – 164.414.
   


(m) **SEC Regulation S-P**: 17 C.F.R. § 248.

(n) **SEC Regulations**: 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

(o) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

2. **Regulations Imposing Authentication Requirements**

   (a) **ACH Operating Rules** (2005) Section 2.10.2.2 (“Verification of Receiver’s Identity”)

   (b) **Banking Know Your Customer Rules**

      i. 31 CFR § 103.121, Customer Identification Programs for banks, savings associations, credit unions, and certain non-Federally regulated banks

      ii. 31 CFR § 103.122, Customer identification programs for broker-dealers

      iii. 31 CFR § 103.123, Customer identification programs for futures commission merchants and introducing brokers

      iv. 31 CFR § 103.131, Customer identification programs for mutual funds


   (e) **USA PATRIOT Act**

      i. 31 U.S.C. 5318 – Section 326 – “Verification of Identification”

      ii. Know your customer rules

   (f) **UN Convention on the Use of Electronic Communications in International Contracts** – Article 9

3. **Data Disposal / Destruction Regulations**

   (a) **FCRA Data Disposal Rules**: 12 C.F.R. Parts 334, 364

   (b) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).
4. Security Breach Notification Regulations


(d) **HIPAA Amendments**: Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), at sections 13401 et. seq


D. State Regulations

1. **Insurance – NAIC Model Regulations**: National Association of Insurance Commissioners, Standards for Safeguarding Consumer Information, Model Regulation.


E. Best Practices Guidelines Issued by Government Agencies


F. Court Decisions


2. **LabMD v. FTC**, No. 16-16270 (11th Cir. June 6, 2018)


G. CFPB Decisions and Consent Decrees re Data Security


H. FTC Decisions and Consent Decrees re Data Security

See list of all FTC Data Security Cases - https://www.ftc.gov/datasetecurity

I. European Union

General Data Protection Regulation (GDPR); http://www.eugdpr.org.

K. Other Countries

1. **Argentina**: Act 25,326, Personal Data Protection Act (October 4, 2000), § 9; Security Measures for the Treatment and Maintenance of the Personal Data Contained in Files, Records, Databanks and Databases, either non state Public and Private (November 2006)


4. **Hong Kong**: Personal Data (Privacy) Ordinance, December 1996, Schedule 1, Principle 4.

5. **Japan**: Act on the Protection of Personal Information, Law No.57, 2003, Articles 20, 21, 22, and 43

6. **South Korea**: The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., Amended by Act No. 7812, December 30, 2005, Articles 28, 29
Chapter 13
Get SMART on Data Protection
Training and How to Create
a Culture of Awareness
Ruth Hill Bro and Jill D. Rhodes

I. Data Protection Training Basics and Core Principles

Any business that works with personal and sensitive data must develop a strategy for protecting that data. When assessing how to do so, organizations, including law firms, often mistakenly rely on technology as the solution. In fact, four factors are key to implementing a proper information security and data protection program in any setting:

- Establishing the appropriate **governance** for the data, such as policies and the oversight of an executive level committee tasked with reducing data protection risk;
- Ensuring that the **people** working with the data know how best to protect it;
- Assessing data protection and usage **processes**; and
- Employing appropriate **technology** to protect the network.

These four factors work together to develop an overarching and effective program.
This chapter focuses on the people aspect of that equation, but other factors (e.g., governance and processes) also come into play. Most data missteps in law firms and other businesses are directly linked to something an employee or contractor did, whether intentionally or unintentionally. The easiest way to address this risk is to educate employees and others about the risk and their role in protecting personal and sensitive data.

Education and training can be provided by many facets of the organization, whether human resources (HR), the chief privacy officer (CPO), the chief information security officer (CISO), or others. Regardless of which groups do the training, it is critical that they work together to produce a common vision and message that is then disseminated across the organization.

A. Why Train on Data Protection?

All organizations, including law firms, are increasingly recognizing that data underpins virtually everything that they do and—like other valuable business assets—should be protected.

The trend is to adopt a reasoned and comprehensive strategy that makes data protection a part of the corporate culture and the job of every individual working for the business (partners, associates, paralegals, interns/law students, information technology (IT), HR, executives, administrators, administrative assistants, and other staff).1 Such an approach is designed to:

- Minimize missteps that can hit the bottom line (costly litigation; time and resources consumed in responding to government, press, or attorney disciplinary commission inquiries or investigations; adverse media coverage; damage to client or customer relationships; and so on), and
- Help businesses achieve a competitive advantage, enhance their profile and image, and enrich their relationship with clients and customers.

1. This trend is in keeping with the “Privacy by Design” (PbD) and “Security by Design” (SbD) movements that are transforming the way that businesses protect data in an information-driven age. See, e.g., Privacy by Design: The 7 Foundational Principles, by Ann Cavoukian, Ph.D., Distinguished Expert-in-Residence, Privacy by Design Centre of Excellence, Ryerson University and former Ontario Privacy Commissioner, at http://www.ryerson.ca/pbdce; see also Fed. Trade Comm’n, Start with Security: A Guide for Business, http://www.ftc.gov/startwithsecurity for insights and guidance on SbD gleaned from over 50 FTC data security settlements.
Yet making data protection a part of the corporate culture is easier said than done:

- Properly addressing data protection issues can require a comprehensive understanding of rapidly changing applicable law in 50 states and territories, at the federal level, and globally (where client or customer data might originate, where third parties might be providing U.S.-based businesses with 24/7 services, etc.). Many laws (particularly for government entities and regulated industries) and lawyers’ professional rules of responsibility expressly or by implication require appropriate data protection training for employees and sometimes contractors as well.²
- Command of the law is not enough, as businesses are often tried in the court of public opinion or are challenged by third-party watchdog groups, regardless of the current legality of the entity’s practices.
- Likewise, technological innovation is occurring at a startling and accelerating pace. The Internet, mobile devices, and ever-more-sophisticated computer technology (all connected to each other and always on) make it easy to collect, analyze, combine, reproduce, and disseminate data, thereby enhancing efficiency and cost-effectiveness but also escalating the risk of making catastrophic mistakes at the speed of light. Yet employees often do not really understand that the latest “smart” technology at work or home (TVs, appliances, toys or gadgets, automated fish tanks, security cameras, digital assistants, voice-controlled smart home hubs, etc.) could be invisibly eavesdropping on confidential discussions using connected microphones, spying via built-in cameras, or providing a new attack vector for accessing the organization’s digital assets.

Change is the watchword, and businesses and their cultures must be nimble in spotting trends and addressing issues that were not even on the radar screen months before.

Business leaders often breathe a sigh of relief once the state-of-the-art security system is installed and comprehensive data protection policies and

². Please see Chapters 4 and 6 of this Handbook for further discussion about the types of legal and professional responsibility requirements placed on lawyers and law firms, which often include education and training.
procedures have been established. Yet notwithstanding adoption of the latest technology and sound data protection principles, businesses are only as strong as their weakest (human) link:

- The disgruntled or downsized “Gen X” employee who has it in for the organization and whose system access was not terminated on the last day of employment.
- The IT director who fails to install patches on a regular basis, thereby leaving networks vulnerable.
- The HR employee who leaves sensitive employee records unlocked or in electronic files with inadequate access restrictions.
- The associate who unwittingly compromises the firm’s client relationships through a lost laptop, phone, or unencrypted flash drive left on an airplane or in a taxi or rideshare vehicle.
- The super-connected, tech-savvy “Millennial” employee who overshares on social media and underestimates how that may sabotage the company’s confidential data.
- The road-warrior employee whose actions (or inaction) regarding the latest mobile technology (including “bring your own device”) may violate internal data security policies or rules of professional responsibility.
- The “Baby Boomer” senior partner who unleashes ransomware by clicking on a link that looks like it came from a colleague or board member.
- The administrative assistant who provides extensive client or firm information after receiving a fraudulent e-mail that appears to be coming from her supervisor or a firm or business executive requesting information.
- The third-party vendor who stores data overseas without appropriate security controls.

Countless studies, audit trails, and surveys over the years have repeatedly confirmed that the biggest data protection threats come from within one’s own organization. Most missteps are unintentional. Many mistakes can be avoided and risks can be minimized with appropriate training and awareness-raising. Yet this is often an overlooked component of data protection initiatives—the missing link when it comes to security.
B. What Does SMART Training Look Like?

What does training actually mean, and what are businesses doing to address data protection’s weakest link? Over the years, this question has been posed to CPOs drawn from various industries, locations, and corporate cultures, and a consistent pattern of answers has emerged. In short, when conducting training, businesses need to be SMART:

- **S**tart training on hiring.
- **M**easure what you do.
- **A**nnually provide training.
- **R**aise awareness and provide updates continually.
- **T**ailor training by role.

In considering these SMART training steps and what they mean for one’s business, it is important to keep in mind that the particular data protection training that is right for one entity is not necessarily right for another, even if they are in the same industry or are law firms of similar size. Businesses differ in many ways—for example, the degree of centralization, their corporate cultures, the jurisdictions in which they operate, their objectives, their resources and budget, their existing data protection infrastructure, their buy-in from senior management, and so on.

1. **S**—Start Training on Hiring

Given the fundamental role of data in everything a business does, training on how to protect that data should start on day one. Data protection training should be provided to all new employees and, increasingly, to contractors as well. In cases where it is not feasible to do such training for all employees initially (due to bandwidth, budget, or other constraints), businesses might choose to focus training on selected employees (e.g., HR personnel and those in key business roles or units).

---

3. Chapter co-author Ruth Hill Bro has posed such training questions since 2005 in her recurring column called *CPO Corner: Interviews with Leading Chief Privacy Officers*, which features 17 questions designed to identify trends and best practices, showcase the diverse range of CPOs, and capture key benchmarking and practical implementation information regarding data protection issues; see interviews posted at ABA, Section of Science & Technology Law: E-Privacy Law Committee, http://www.ambar.org/eprivacy.
In the employee context, training is provided as a part of employee orientation. Such training can take different forms, using a variety of media:

- An initial in-person, instructor-led session (large group, small group, or one-on-one, as appropriate), which can encourage interaction (but may not always be scalable or practical for some organizations in all situations), and/or
- An intranet/computer-based training module.

Coverage can include a wide range of topics, including:

- High-level overviews applicable to all employees and contractors;
- Instruction on relevant data protection laws and regulations (and professional rules of responsibility, where applicable), internal policies and procedures, fundamentals of the relevant technology, and industry best practices;
- Protecting confidentiality and security of data; and
- Steps to take when addressing a suspected data breach.

Such training should be coordinated with other training (regarding records management, code of conduct, etc.) and should be reviewed to avoid contradictions and conflicts in approach and message. Consideration should be given to whether the time, format, and content are suitable across different parts of the organization. Issues of translation, local law, and local customs can come into play here as well.

2. Measure What You Do
Measurement and assessment are a core component of many of these initial training sessions as well as in follow-up training. Administering tests (e.g., a graded online quiz) can help to confirm understanding and gauge the overall effectiveness of the training; it can also help to ensure that the work has actually been done. For example, employees and contractors could be required to correctly answer four of five assessment questions at the end of each training section. Broader measurements—such
as comparisons of incidents and types of missteps before and after training—can also help businesses to make training more effective while demonstrating return on investment (which can be important in making the case for budget).

3. **A—Annually Provide Training**
   It is prudent (and in some cases required under applicable law, rules, or policies) to ensure that employees annually receive a data protection training update, along with corresponding assessments or tests. Where relevant, certification or continuing legal education (CLE) or professional responsibility credit could be provided, thereby offering an additional incentive to do the training. Such follow-up instruction is often computer-based, so it can be deployed to diverse geographic locations and in a time frame that is convenient for the person receiving the training. Sometimes these annual updates are a part of annual recertification regarding business conduct guidelines.

4. **R—Raise Awareness and Provide Updates Continually**
   It is impossible to integrate appropriate data security practices into a culture by using just introductory training on hiring and mandatory annual training. To address this, businesses need to look for ways to raise data awareness and update employees on data protection on an ongoing basis. This is due to a number of factors, including the speed with which the issues change, the different ways in which people learn, the need for reinforcement, and so on. With ongoing awareness-raising, law firms and other businesses can integrate information security practices in such a way that they become as commonplace as turning on a computer.

5. **T—Tailor Training by Role**
   Going beyond high-level, one-size-fits-all training allows for training to be tailored to focus on specific roles of individuals, different generational challenges, and specific requirements for contractors and third parties. Tailoring of data protection training can take various forms, depending on the organization:
• Start with a Data Protection 101 online course that is available on demand (successfully completing it results in a certificate). The basic module can then be supplemented by training and awareness-raising specific to role (HR, those involved heavily in data handling, contractors, product design, engineering, sales, senior executives, lawyers, paralegals, administrative assistants, etc.), business unit, geographic location, and the like.

• Determine who should receive direct training from, or at least meet in person with, the CPO, CISO, CIO or IT director, legal counsel, or other qualified trainers. It is helpful for those tasked with training to meet with selected employees to learn about their data practices and then tailor training efforts accordingly. For example, some CPOs meet regularly with the company’s engineering, product design, and sales teams to raise important issues in planning meetings and gain insights to develop appropriate training.

• Ask data protection officers (or other relevant individuals) associated with the business lines to develop training and tools to enable the application of data protection policies to their respective areas.

• Hire specialists, internally or externally, to refine and enhance training efforts.

• Not all training and awareness-raising comes from within. Small firms or solo practitioners, those who lack specialized staff, and others looking for cost-effective approaches should take advantage of online training modules, relevant CLE courses and conferences, resources offered by bar associations (the American Bar Association and the ABA’s Sections, Divisions, and Forums; state and local bar associations; specialty bar associations; etc.), training publications, and the like.

• As noted above, training for some roles (e.g., lawyers) may be accompanied by certification or CLE or professional responsibility credit.

Businesses that use SMART training can provide the missing link that will help make data protection a part of the culture and turn their employees into one of their strongest links when it comes to protecting one of the most valuable assets of any business.
II. SMART Training in Action

Implementing a SMART training program does not have to be complicated or require significant budget. The program pays for itself by reducing the risk of data loss and increasing awareness about data protection.

A. Understanding the Basics of Employees: Role and Generational Differences

First, any training program should assess and understand the recipients of the training. As mentioned above, the role of the employee in the organization will make a difference in the type of training received. An associate working with e-discovery matters and technology every day will have different considerations than a mail clerk or even other associates and partners in the firm.

In addition, generational differences play a role in how training should be developed, the type of training and communication that a person prefers to receive, and how best to provide the training. Cam Marston, in his practical and often humorous book Generational Insights: Practical Solutions for Understanding and Engaging a Generationally Disconnected Workforce,\textsuperscript{4} discusses how each generation differs in its approach to learning:

- **Baby Boomers** (born 1946–1964) tend to continue to hold key leadership positions (e.g., partners) in the organization. They focus on work ethic and often measure it in terms of hours spent, rather than productivity. They value face time and relationships and seek loyalty. They look for those willing to put in whatever time is necessary to complete the task and support the team.\textsuperscript{5} When training Baby Boomers, it is critical to include preevaluation of technology skills and training that is participatory but not intimidating.\textsuperscript{6}

- **Generation Xers** (born 1965–1979) often have a more entrepreneurial spirit and are focused on challenging or reinventing the status quo.

\textsuperscript{4} Cam Marston, Generational Insights: Practical Solutions for Understanding and Engaging a Generationally Disconnected Workforce (2010).
\textsuperscript{5} Id. at 33–34.
\textsuperscript{6} Id. at 39.
They tend to seek open communication, no matter their title or status. Unlike Baby Boomers, Gen Xers focus on productivity rather than time. They often seek a person, not a company, where their loyalty will lie. Training programs should address the Gen X employee’s career goals and be flexible, providing options and choices. For Gen Xers to see training as valuable, senior-level management must demonstrate its commitment to the training as valuable.

- **Millennials** (born 1980–2000) tend to be the most idealistic of the three groups. Unlike Gen Xers, who prefer to work independently with few checkpoints, Millennials want constant communication and positive reinforcement and prefer regular checkpoints at each phase of their work. Training programs for Millennials need to be group-oriented (where practical), interactive, and fun. They prefer that everyone be allowed to take a role in some part of the teaching as well as the learning.

Given the diverse nature of the workforce and the different means by which people learn and absorb information, any training or education campaign must integrate a variety of employee perspectives and capabilities and incorporate a variety of approaches.

### B. Building an Effective and Diverse Program

Leveraging the SMART principles described above, any organization can quickly and easily build an ongoing training and education campaign.

First, it is critical to make the campaign fun and creative. While the message of data protection is serious, the delivery does not need to be. People of all generations tend to learn more through consistent messaging that has a direct impact on their lives. Those working on the data protection training should develop easy, fun, and catchy slogans that employees will remember.

---

7. *Id.* at 35.
8. *Id.* at 41.
9. *Id.* at 35, 37.
10. *Id.* at 42.
One example is the SAFE program,\(^\text{11}\) an information security awareness program that was developed for Option Care Enterprises, Inc. as a way to help employees remember how best to protect and secure sensitive information:

Secure the organization’s data: Where are you storing client data? How are you deleting it?

Asset protection: Do you know where your computer/iPad/phone is?

Friend or Foe: Who is sending you an e-mail? Is it something you expected or phishing?

Encrypt: Are you encrypting sensitive e-mails before sending them out?

A program such as SAFE can be used throughout the year to educate staff; different themes within each of the four SAFE categories above can be featured.

Next, identify something, such as a mascot, that represents the organization and symbolizes data protection to help lighten the delivery of a serious message. For example, Option Care, which provides infusion services to patients in their homes, uses a mascot named “The Infuser.”

The Infuser’s motto is “Infusing Security into Everything We Do.” Every time employees see this mascot and message, they are reminded about protecting sensitive information. It is a fun, easy, and quick cue that costs very little to the organization to develop and implement.

Third, ensure that training is continuous, and use various methods to implement it. In addition to mandatory training at specific times (when employees join the organization and subsequent annual training), continuous education is key to any successful cultural transformation. The following are some ideas to keep the momentum going:

---

11. The SAFE program was developed by Option Care CISO Jill Rhodes, who is also an author of this chapter and co-editor of this Handbook. For further information on the program, contact Ms. Rhodes at jill.rhodes@optioncare.com.
Leverage current newsletters, and place brief articles within them that discuss data protection.

Conduct e-mail campaigns (monthly or as needed) with data protection guidelines, relevant media coverage, and so on to remind everyone (or otherwise make them aware) of relevant policies and practices.

Offer periodic “Data Protection Awareness Weeks” or “Security Awareness Drives” with guest speakers and other special events.

Strategically place wall posters and other communications that promote data protection.

Publish monthly articles on the company and line-of-business intranet home pages to raise data protection awareness.

Send periodic e-mails to highlight ongoing opportunities for online training and in-person sessions conducted by members of the data protection team or outside speakers.

Develop white papers and other material related to relevant data protection topics (aiming for greater frequency and detail over time).

Remind employees that data protection training is an important part of their job by including it as a factor in their annual performance evaluation; celebrate successes and reward those who meet the objectives (and, if needed, identify opportunities for growth and improvement).

Fourth, involve employees directly. Hold data protection competitions between divisions, offices, or floors in a building with the goal of identifying an employee/group activity that protected the organization’s information in a noteworthy way. Recognize the individual or group winners, name them in the monthly newsletter or blog, and provide a pizza lunch for the winner—the more recognition, the better.

Build an ambassador/liaison or similar program across the organization. Whether it is by office, region, subject matter expertise, or business unit, identify a way to have a data protection representative in each. Although senior leadership is important, the representative should be a mid-level employee who still has influence with peers, subordinates, and leadership. Meet with the data protection ambassadors/liaisons regularly to discuss data protection issues and (in line with the discussion about Millennials above) ensure that they are a part of the solution by having them serve as
the leaders who will train and educate the employees they work with on a regular basis.

Educate employees about how to protect data at home as well as in the workplace. Data protection does not start when a person logs into the network or end when she shuts down for the evening. Everyone’s family members and friends are constantly touching sensitive and/or personal digital data. Whether it is through social media or new mobile apps, data is being collected. By educating employees to protect data in all facets of their lives, they will approach data protection more holistically in their daily work life.

All of these methods are easy, cheap, fun, and effective ways to communicate and educate employees about enhancing data protection in the organization. As noted earlier, it is critical to find ways to measure the success of these campaigns (the “M” in “SMART” training).

C. Measuring Success (Through Phishing Campaigns and Other Means)

One of the easiest ways to measure the success of a campaign is to test employees by phishing them directly. Phishing normally occurs when a malicious e-mail is sent either directly to an individual (spear phishing) or to many in the hope that the target will click on a link within the e-mail and then spread a virus that could infect the individual’s computer, at a minimum, or the entire enterprise network. Ransomware, discussed throughout this Handbook, has often been caused by phishing.

As part of a SAFE campaign (Friend or Foe), organizations can implement their own company-wide phishing campaign, sending “malicious” e-mails to employees, as someone trying to harm the organization would do. When an employee clicks on the e-mail, instead of infecting the system, the employee receives an educational message about the phishing e-mail and the fact that had it been real, harm could have come to the organization. This type of campaign measures the click rate and, when conducted regularly, can be used to monitor those who are clicking regularly. As a result, specific training can be developed for those individuals or groups. Phishing programs provide a quantitative measurement related to security awareness.

Reporting numbers also can provide both quantitative and qualitative opportunities for measuring success. As more training and education occurs, the number of incidents reported to appropriate leadership will also increase.
Increased reporting could be anything from the reporting of a specific data breach or loss incident to reporting of phishing e-mails. As these incidents are tracked, greater information becomes available about employee knowledge and understanding of data protection.

In the end, a data breach or loss will most likely occur as a result of something an employee did or did not do. The best way to prevent such missteps is to educate the people in the organization about how they can better protect the information around them.

III. Ten Key Points

1. Make data protection a part of the corporate culture and the job of every individual.
2. Recognize that the biggest risks to data come from the people working for the organization and that training and raising awareness are essential to reducing those risks.
4. Recognize that one size doesn’t fit all; it is important to undertake training that fits a business’s own needs.
5. Build a program that represents the organization’s employees both from a role perspective and a generational one.
6. Make any training campaign fun and interesting—let the employees lead it through ambassador/liaison programs and in other ways.
7. Train employees on how to protect information in all facets of their lives, not just in the workplace. By helping them protect their family and friends at home, they will further integrate these practices at work.
8. Reward! Reward! Reward! Use competitions with prizes to further induce employees to become more aware and supportive of data protection across the organization.
9. Measure success through phishing programs and tracking of reporting of incidents and responses.
10. Know that training and awareness-raising is a never-ending journey (not a destination) that can require changes in direction in response to changes in the law, technology, media coverage, and one’s own experiences and new business initiatives. Adapt accordingly, while keeping message delivery mechanisms light and easy to understand for all of the people who work for the organization.
Lawyers’ Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

1 See, e.g., Dan Steiner, Hackers Are Aggressively Targeting Law Firms’ Data (Aug. 3, 2017), https://www.cio.com (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”). See also Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).


opinion picks up where Opinion 477R left off, and discusses an attorney’s ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney’s ethical obligations after a data breach, and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules per se represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney’s roles, level of authority, and responsibility in the law firm’s operations.

6 The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a “firm.” A “firm” is defined in Rule 1.0(c) as “a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization.” How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer’s position in the firm. See Model Rules of Prof’l Conduct R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); Model Rules of Prof’l Conduct R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and Model Rules of Prof’l Conduct R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

7 In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.”) See also, e.g., Cybersecurity Resources, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).
I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.

10 ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”
In the context of a lawyer’s post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission’s thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer’s competency in this regard may be satisfied either through the lawyer’s own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.\textsuperscript{11}

1. **Obligation to Monitor for a Data Breach**

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers’ offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer’s systems, destroying the lawyer’s infrastructure on which confidential information resides and incapacitating the attorney’s ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred, whether further action is warranted, whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties, and how and when the lawyer must take further action under other regulatory and legal provisions. Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

---

14 MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).
15 See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).
16 The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.\textsuperscript{18} The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”\textsuperscript{19} While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm’s network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

\textsuperscript{18} See ABA CYBERSECURITY HANDBOOK, supra note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.  

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer’s clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.” These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer’s office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer’s duty of communication and honesty under

---

21 We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer’s computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.
Model Rules 1.4 and 8.4(c). Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer’s efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise. The 2012 modification added a duty in paragraph (c) that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

22 The rules against dishonesty and deceit may apply, for example, where the lawyer’s failure to make an adequate disclosure or any disclosure at all amounts to deceit by silence. See, e.g., MODEL RULES OF PROF’L CONDUCT R. 4.1 cmt. [1] (2018) (“Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.”).
23 MODEL RULES OF PROF’L CONDUCT R. 1.6(a) (2018).
24 Id. at (c).
• the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).  

As this Committee recognized in ABA Formal Opinion 477R:

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney’s competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.  

Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.  

As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.  

---

25 MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, supra note 9, at 5.

26 ABA CYBERSECURITY HANDBOOK, supra note 11, at 122.

27 MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”)

28 ABA CYBERSECURITY HANDBOOK, supra note 11, at 73.
Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.\(^{29}\) In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer’s Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.\(^{30}\) We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.\(^{31}\)


\(^{30}\) This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

\(^{31}\) Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass’n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients’ confidential information,
Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”\(^{32}\) The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).\(^{33}\)

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer’s ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client’s interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.\(^{34}\)

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4’s requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.


\(^{33}\) Id.

\(^{34}\) MODEL RULES OF PROF’L CONDUCT R. 1.4(b) (2018).
Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer . . . .” Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.”

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.
2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.” When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9. We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely. Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absence an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

36 See Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).
the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.39

3. Breach Notification Requirements

The nature and extent of the lawyer’s communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the “safe harbor” provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer’s office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer’s plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients’

39 Cf. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).
information. Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer’s obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws. Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information. Most breach notification laws specify who must comply with the law, define “personal information,” define what constitutes a breach, and provide requirements for notice. Many federal and state agencies also have confidentiality and breach notification requirements. These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual’s relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer’s possession that was accessed by an unauthorized user.

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make “reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

42 Id.
43 Id.
44 ABA CYBERSECURITY HANDBOOK, supra note 11, at 65.
45 Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.
breach under Model Rule 1.4 in sufficient detail to keep clients “reasonably informed” and with an explanation “to the extent necessary to permit the client to make informed decisions regarding the representation.”
Ethical Obligations Related to Disasters

The Rules of Professional Conduct apply to lawyers affected by disasters. Model Rule 1.4 (communication) requires lawyers to take reasonable steps to communicate with clients after a disaster. Model Rule 1.1 (competence) requires lawyers to develop sufficient competence in technology to meet their obligations under the Rules after a disaster. Model Rule 1.15 (safekeeping property) requires lawyers to protect trust accounts, documents and property the lawyer is holding for clients or third parties. Model Rule 5.5 (multijurisdictional practice) limits practice by lawyers displaced by a disaster. Model Rules 7.1 through 7.3 limit lawyers’ advertising directed to and solicitation of disaster victims. By proper advance preparation and planning and taking advantage of available technology during recovery efforts, lawyers can reduce their risk of violating the Rules of Professional Conduct after a disaster.

Introduction

Recent large-scale disasters highlight the need for lawyers to understand their ethical responsibilities when those events occur. Extreme weather events such as hurricanes, floods, tornadoes, and fires have the potential to destroy property or cause the long-term loss of power. Lawyers have an ethical obligation to implement reasonable measures to safeguard property and funds they hold for clients or third parties, prepare for business interruption, and keep clients informed about how to contact the lawyers (or their successor counsel). Lawyers also must follow the advertising rules if soliciting victims affected by a disaster.

Much information is available to lawyers about disaster preparedness. The American Bar Association has a committee devoted solely to the topic and provides helpful resources on its website. These resources include practical advice on (i) obtaining insurance, (ii) types and methods of information retention, and (iii) steps to take immediately after a disaster to assess damage and rebuild. Lawyers should review these and other resources and take reasonable steps

---

1 This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.
Formal Opinion 482

to prepare for a disaster before one strikes the communities in which they practice. Lawyers should also review their disaster preparedness plans when a disaster threatens. Included within disaster planning, and of particular importance for sole practitioners, is succession planning so that clients and others know where to turn if a lawyer dies, is incapacitated, or is displaced by a disaster.

Despite the wealth of information available on preparing for a disaster and on the practical steps a lawyer should take to preserve the lawyers’ and the clients’ property and interests after a disaster, there is a dearth of guidance on a lawyer’s ethical responsibilities (i) when a disaster threatens, and (ii) after a disaster occurs. This opinion addresses the lawyers’ obligations in these circumstances.

A. Communication

Model Rule 1.4 requires lawyers to communicate with clients. One of the early steps lawyers will have to take after a disaster is determining the available methods to communicate with clients. To be able to reach clients following a disaster, lawyers should maintain, or be able

---

3 There are three ethics opinions from state bars on a lawyer’s obligations after a disaster: N.Y. City Bar Ass’n Formal Op. 2015-6 (2015) advises lawyers to notify clients of destruction of client files in a disaster if the destroyed documents have intrinsic value (such as a will) or if the lawyer knows the client may need the documents; La. Advisory Op. 05-RPCC-005 (2005) advises lawyers on providing pro bono assistance through a hotline or both; and State Bar of Cal. Standing Comm. on Prof’l Responsibility & Conduct, Formal Op. 2004-166 (2004) advises lawyers not to participate in a mass disaster victims chat room because it is intrusive, but not because it is prohibited as in-person solicitation.

4 This opinion focuses primarily on the obligations of managers and supervisors within the meaning of Rule 5.1, recognizing that lawyers practice in a variety of contexts, including solo offices, small firms, large firms, government agencies and corporate offices. Subordinate lawyers may rely on the reasonable decisions of managers and supervisors on how to address the ethical obligations this opinion describes. Some of the obligations may be reasonably delegated or assigned to specific lawyers within a firm or organization. Methods of compliance with the obligations may vary depending on the practice context in which they arise. In addition, lawyers employed by governmental or other institutional entities may be subject to requirements imposed by law, or the policies of those entities. Reasonable implementation of the obligations described in this opinion satisfies the Model Rules. Opinion 467 provides examples of how to comply with obligations under several Model Rules in a variety of practice settings. See ABA Comm’n on Ethics & Prof’l Responsibility, Formal Op. 467 (2014).

5 MODEL RULES OF PROF’L CONDUCT R. 1.4 (2018) provides:

(a) A lawyer shall:
(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
(3) keep the client reasonably informed about the status of the matter;
(4) promptly comply with reasonable requests for information; and
(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.
to create on short notice, electronic or paper lists of current clients and their contact information. This information should be stored in a manner that is easily accessible.  

In these early communications clients will need to know, for example, if the lawyer remains available to handle the client’s matters, or, alternatively, if the lawyer is unavailable because of the disaster’s effects, and may need to withdraw. In a situation in which a disaster is predicted, for example, with a hurricane or other extreme weather event, lawyers should consider providing clients with methods by which the lawyer may be reached in the event that emergency communication is necessary. Information about how to contact the lawyer in the event of an emergency may be provided in a fee agreement or an engagement letter.  

In identifying how to communicate with clients under these circumstances, lawyers must be mindful of their obligation under Rule 1.1 to keep abreast of technology relevant to law practice and Rule 1.6(c)’s requirement “to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.”  

6 This opinion addresses a lawyer’s ethical responsibilities. Lawyers should take similar steps to maintain communication with their own colleagues and staff. It is also good practice for a lawyer to maintain and update this information on a secure Internet website after the disaster so that colleagues and support staff will have a centralized location to find contact information. For information about the appropriate methods for storing electronic or paper records, lawyers may consult the ABA Committee on Disaster Response and Preparedness website. Also, many state bars and courts provide information on disaster preparedness.

7 Practical problems a lawyer may wish to consider in advance include whether (i) landline phones will be out of service, (ii) the U.S. Postal Service will be impaired, and (iii) electronic devices will lose battery power.  

8 ABA Model Rule 1.1 provides, “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” Comment [8] to Rule 1.1 provides: “. . . [A] lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . .”  

B. Continued Representation in the Affected Area

Lawyers who continue to provide legal services in the area affected by a disaster have the same ethical obligations to their clients as before the disaster, although they may be able to provide advice outside their normal area of expertise.  

Lawyers may not be able to gain access to paper files following a disaster. Consequently, lawyers must evaluate in advance storing files electronically so that they will have access to those files via the Internet if they have access to a working computer or smart device after a disaster. If Internet access to files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer.  

10 Comment [3] to Rule 1.1 allows: “In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances. Ill-considered action under emergency conditions can jeopardize the client's interest.”  

11 Rule 1.15 requires that lawyers take reasonable steps to preserve trust account records and documents and property of clients and third parties when a lawyer has notice of an impending disaster. See also subsection (E), infra, for a discussion of a lawyer’s obligations when files are lost or destroyed in a disaster.  

12 Lawyers must understand that electronically stored information is subject to cyberattack, know where the information is stored, and adopt reasonable security measures. They must conduct due diligence in selecting an appropriate repository of client information “in the cloud.” Among suggested areas of inquiry are determining legal standards for confidentiality and privilege in the jurisdiction where any dispute will arise regarding the cloud computing services. See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (May 22, 2017) (Lawyer may send client information over the Internet if lawyer makes reasonable efforts to prevent inadvertent or unauthorized access, but may be required to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security); Ala. State Bar Op. 2010-02 (2010) (Lawyer may outsource storage of client files through cloud computing if they take reasonable steps to make sure data is protected); State Bar of Ariz. Formal Op. 09-04 (2009) (Lawyer may use online file storage and retrieval system that enables clients to access their files over the Internet, as long as the firm takes reasonable precautions to protect the confidentiality of the information; in this case, proposal would convert files to password-protected pdf documents that are stored on a Secure Socket Layer server (SSL) which encodes the documents); State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2012-184 (2012) (Lawyer may operate virtual law office "in the cloud" as long as the lawyer complies with all ethical duties such as confidentiality, competence, communication, and supervision; lawyer should check vendor credentials, data security, how information is transmitted, whether through other jurisdictions or third-party servers, the ability to supervise the vendor; and the terms of the contract with the vendor); Fla. Bar Op. 12-3 (2013) (Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely); Ill. State Bar Ass’n Op. 16-06 (2016) (Lawyer may use cloud-based service to store client files as long as the lawyer "takes reasonable measures to ensure that the client information remains confidential and is protected from breaches"; lawyer should engage in due diligence in choosing the provider, including reviewing industry norms, determining the provider's security precautions such as firewalls, password protection and encryption, the provider's reputation and history, asking about any prior breaches, requiring that the provider follow confidentiality requirements, requiring that the data is under the lawyer's control, and requiring reasonable access if the contract terminates or the provider goes out of business); Iowa State Bar Ass’n Op. 11-01 (2011) (Due diligence a lawyer
As part of the obligation of competence under Rule 1.1 and diligence under Rule 1.3, lawyers who represent clients in litigation must be aware of court deadlines, and any extensions granted due to the disaster. Courts typically issue orders, usually posted on their websites, addressing extensions.\textsuperscript{13} Lawyers should check with the courts and bar associations in their jurisdictions to determine whether deadlines have been extended.

Lawyers also must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust. A lawyer’s obligations with respect to these funds will vary depending on the circumstances. Even before a disaster, all lawyers should consider (i) providing for another trusted signatory on trust accounts in the event of the lawyer’s unexpected death, incapacity, or prolonged unavailability and (ii) depending on the circumstances and jurisdiction, designating a successor lawyer to wind up the lawyer’s practice.\textsuperscript{14} Lawyers with notice of an

\begin{itemize}
\item should perform before storing files electronically with a third party using SaaS (cloud computing) includes whether the lawyer will have adequate access to the stored information, whether the lawyer will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider; State Bar of Nev. Formal Op. 33 (2006) (Lawyer may store client files electronically on a remote server controlled by a third party as long as the firm takes precautions to safeguard confidential information such as obtaining the third party's agreement to maintain confidentiality); New York City Bar Report, The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations (Nov. 2013), https://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf; N.Y. State Bar Ass’n Op. 842 (2010) (Permission to use an online computer data storage system to store client files provided the attorney takes reasonable care to maintain confidentiality; lawyer must stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); State Bar Ass’n of N.D. Advisory Op. 99-03 (1999) (Permission to use electronic online data service to store files as long as the lawyer properly protects confidential client information, perhaps via password protected storage); Pa. Bar Ass’n Op. 2011-200 (2011) (“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”); S.C. Bar Advisory Op. 86-23 (1988) (A lawyer can store files in a storage facility operated by a third party if the lawyer ensures that confidentiality is maintained); Tenn. Formal Op. 2015-F-159 (2015) (Lawyer may store information in the cloud if the lawyer takes reasonable measures to protect the information); Vt. Advisory Op. 2010-6 (2010) (Lawyers may use cloud computing if they take reasonable steps to ensure confidentiality of information and that information is accessible).
\item See MODEL RULES OF PROF’L CONDUCT R. 1.1 & 1.3 (2018). Designating a successor and adding trusted signatories are good practices that may already be in place as part of normal succession planning. Some states require designation of a successor counsel or inventory lawyer. See, e.g., Rules Regulating the Fla. Bar R. 1-3.8(e),
impending disaster should take additional steps. For example, a transactional lawyer should review open files to determine if the lawyer should transfer funds to a trust account that will be accessible after the disaster or even attempt to complete imminent transactions prior to the disaster if practicable.

A disaster may affect the financial institution in which funds are held, or the lawyer’s ability to communicate with the financial institution. Consequently, lawyers should take appropriate steps in advance to determine how they will obtain access to their accounts after a disaster. Different institutions may have varying abilities to recover from a disaster. After a disaster, a lawyer must notify clients or third persons for whom the lawyer is holding funds when required disbursements are imminent and the lawyer is unable to access the funds, even if the lawyer cannot access the funds because the financial institution itself is inaccessible or access is beyond the lawyer’s capability.

C. Withdrawal from Representation After a Disaster

Lawyers whose circumstances following a disaster render them unable to fulfill their ethical responsibilities to clients may be required to withdraw from those representations. Rule 1.16(a)(1) requires withdrawal if representation will cause the lawyer to violate the rules of professional conduct. Rule 1.16(a)(2) requires withdrawal if “the lawyer’s physical or mental condition materially impairs the lawyer’s ability to represent the client,” for example, if the lawyer suffers severe injury or mental distress due to the disaster. Rule 1.16(b)(7) allows termination of the representation when the lawyer has “other good cause for withdrawal.” These conditions may be present following a disaster. In determining whether withdrawal is required, lawyers must assess whether the client needs immediate legal services that the lawyer will be unable to timely

---

Iowa Ct. Rule 39.18(1), Me. Bar R. 32(a), and Mo. R. 4-1.3 cmt. [5] & R. 5.26. Some states permit voluntary designation, including California, Delaware, Idaho, South Carolina, and Tennessee. See Mandatory Successor Rule Chart (June 2015), ABA, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mandatory_successor_rule_chart.authcheckdam.pdf. Lawyers should also be aware that, in most jurisdictions, a power of attorney to handle law firm affairs will be insufficient because it expires on the principal’s death.

15 The rules do not require a lawyer to place funds in a large or national financial institution. See MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018). However, a prudent lawyer in a disaster-prone area should inquire about a financial institution’s disaster preparedness before placing funds there. The lawyer must comply with IOLTA requirements regardless of which financial institution the lawyer chooses.

provide. Lawyers who are unable to continue client representation in litigation matters must seek the court’s permission to withdraw as required by law and court rules.\textsuperscript{17}

D. Representation of Clients by Displaced Lawyers in Another Jurisdiction

Some lawyers may either permanently or temporarily re-locate to another jurisdiction following a disaster. Their clients and other residents of the lawyers’ home jurisdiction may relocate to the same jurisdiction, or elsewhere, and still require legal services. Although displaced lawyers may be able to rely on Model Rule 5.5(c) allowing temporary multijurisdictional practice to provide legal services to their clients or displaced residents, they should not assume the Rule will apply in a particular jurisdiction. Comment [14] to Rule 5.5 provides:

\textit{\ldots lawyers from the affected jurisdiction [by a major disaster] who seek to practice law temporarily in another jurisdiction, but in which they are not otherwise authorized to practice law, should consult the Model Court Rule on Provision of Legal Services Following Determination of Major Disaster.}

Displaced lawyers who wish to practice law in another jurisdiction may do so only as authorized by that other jurisdiction. Subdivision (c) of the ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster provides:

\textit{Following the determination of a major disaster in another United States jurisdiction, a lawyer who is authorized to practice law and who principally practices in that affected jurisdiction, and who is not disbarred, suspended from practice or otherwise restricted from practice in any jurisdiction, may provide legal services in this jurisdiction on a temporary basis if permitted by order of the highest court of the other jurisdiction. Those legal services must arise out of and be reasonably related to that lawyer’s practice of law in the jurisdiction, or area of such other jurisdiction, where the major disaster occurred.}\textsuperscript{18}

This ABA Model Court Rule further provides that lawyers:

- are required to register with the Supreme Court in the state where they are temporarily allowed to practice;

\textsuperscript{17} \textsc{Model rules of prof’l conduct R. 1.16(c)} (2018).
\textsuperscript{18} Full text of the ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster (2007) can be found at: \url{https://www.americanbar.org/content/dam/aba/migrated/2011_build/professional_responsibility/model_rule_disaster_katrina.authcheckdam.pdf}. The ABA Standing Committee on Client Protection Chart on State Implementation of the ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster (Sept. 8, 2017) can be found at: \url{https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/katrina_chart.authcheckdam.pdf}. 
• are subject to the disciplinary authority in the jurisdiction of the Supreme Court in the state where they are temporarily allowed to practice; and

• must cease practice within 60 days after the Supreme Court in the state where they are temporarily allowed to practice determines the conditions of the disaster have ended.19

E. Loss of Files and Other Client Property

Some lawyers located in an area affected by a disaster may have their files destroyed. Lawyers who maintain only paper files or maintain electronic files solely on a local computer or local server are at higher risk of losing those records in a disaster. A lawyer’s responsibilities regarding these files vary depending on the nature of the stored documents and the status of the affected clients.

Under the lawyer’s duty to communicate, a lawyer must notify current clients of the loss of documents with intrinsic value, such as original executed wills and trusts, deeds, and negotiable instruments.20 Lawyers also must notify former clients of the loss of documents and other client property with intrinsic value. A lawyer’s obligation to former clients is based on the lawyer’s obligation to safeguard client property under Rule 1.15.21 Under the same Rule, lawyers must

19 See ABA Model Court Rule Provision of Legal Services Following Determination of Major Disaster, supra note 17. For an example, see the emergency order entered by the Supreme Court of Texas in 2017, permitting the temporary practice of Texas law by lawyers displaced from their home jurisdictions after Hurricane Harvey. The Court adopted requirements and limitations similar to those in the ABA Model Court Rule. See Court of Texas Amended Emergency Order After Hurricane Harvey Permitting Out-of-State Lawyers to Practice Texas Law Temporarily, Misc. Docket No. 17-9101 (Aug. 30, 2017), available at http://www.txcourts.gov/media/1438820/179101.pdf.

20 See MODEL RULES OF PROF’L CONDUCT R. 1.4 (2018); N.Y. City Bar Ass’n Formal Op. 2015-6 (2015); See also ABA Comm. on Ethics & Prof’l Responsibility, Informal Op. 1384 (1977) (Lawyer should not dispose of client property without client consent, should not destroy information that would be useful to the client if the statute of limitations has not run, should not destroy information that the client may need and is not otherwise easily accessible by the client, should exercise discretion in determining which information might be particularly sensitive or require longer retention than others, should retain trust account records, should protect confidentiality in the destruction of any files, should review files before destruction to determine if portions should be retained, and should retain an index of destroyed files); State Bar of Cal. Standing Comm. on Prof’l Responsibility & Conduct, Formal Op. 2001-157 (2001) (Regarding destruction of closed files, indicating that property of the client such as original documents (like wills) is subject to bailment law or other statute, lawyers may not destroy other file materials without making reasonable efforts to obtain client consent, lawyers may not destroy items required to be retained by law, lawyers may not destroy items if destruction would prejudice the clients’ interests, and criminal case files should not be destroyed while the client is living); State Bar of Mich. Op. R-12 (1991) (Lawyers must give notice to clients regarding file destruction after 1998, files before 1998 may not be destroyed without reasonable efforts to notify the client, and lawyers are not required to notify clients of file destruction if the lawyer maintains a copy of the documents on microfilm (excluding original documents of the client or if destruction of the documents would prejudice the client’s interests)). Lawyers should note that in some states, the client may be entitled to all substantive documents in the file at the client’s request. See e.g., State Bar of Ariz. Op. 15-02 (2015).

21 See also N.Y. City Bar Ass’n Formal Op. 2015-6 (2015).
make reasonable efforts to reconstruct documents of intrinsic value for both current and former clients, or to obtain copies of the documents that come from an external source.\textsuperscript{22}

A lawyer need not notify either current or former clients about lost documents that have no intrinsic value, that serve no useful purpose to the client or former client, or for which there are electronic copies. The lawyer must respond honestly, however, if asked about those documents by either current or former clients.\textsuperscript{23}

The largest category of documents will fall in the middle; i.e., they are necessary for current representation or would serve some useful purpose to the client. For current clients, lawyers may first attempt to reconstruct files by obtaining documents from other sources. If the lawyer cannot reconstruct the file, the lawyer must promptly notify current clients of the loss. This obligation stems from the lawyer’s obligations to communicate with clients and represent them competently and diligently.\textsuperscript{24} A lawyer is not required either to reconstruct the documents or to notify former clients of the loss of documents that have no intrinsic value, unless the lawyer has agreed to do so despite the termination of the lawyer-client relationship.\textsuperscript{25}

ABA Model Rule 1.15(a) also requires lawyers to keep complete records accounting for funds and property of clients and third parties held by the lawyer and to preserve those records for five years after the end of representation. A lawyer whose trust account records are lost or destroyed in a disaster must attempt to reconstruct those records from other available sources to fulfill this obligation.

To prevent the loss of files and other important records, including client files and trust account records, lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly.\textsuperscript{26} Although not required, lawyers may maintain these files solely as electronic files, except in instances where law, court order, or agreement require maintenance of paper copies, and as long as the files are readily accessible and not subject to inadvertent

\textsuperscript{22} Lawyers should consider returning all original documents and documents with intrinsic value created by the lawyer as a result of the representation to clients at the end of representation to avoid this situation.

\textsuperscript{23} See Model Rules of Prof’l Conduct R. 8.4(c) (2018); N.Y. City Bar Ass’n Formal Op. 2015-6 (2015).

\textsuperscript{24} See Model Rules of Prof’l Conduct R. 1.1, 1.3 & 1.4 (2018); N.Y. City Bar Ass’n Formal Op. 2015-6 (2015).

\textsuperscript{25} Lawyers should consider including in fee agreements or engagement letters the understandings between the lawyer and the client about how the lawyer will handle documents once the representation is ended. In addition, lawyers should consult statutes, common law, and court rules that may also govern the retention of client files.

\textsuperscript{26} Model Rules of Prof’l Conduct R. 1.1 (2018); Model Rules of Prof’l Conduct R. 1.3 (2018).
modification or degradation.\textsuperscript{27} As discussed above, lawyers may also store files “in the cloud” if ethics obligations regarding confidentiality and control of and access to information are met.

\textsuperscript{27} ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (May 22, 2017) (Lawyer may send client information over the Internet if lawyer makes reasonable efforts to prevent inadvertent or unauthorized access, but may be required to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security); ABA Comm. on Ethics & Prof’l Responsibility, Informal Op. 1127 (1970) (Lawyers may use company that stores attorney files on computer as long as the company is set up so that the material is available only to the particular attorney to whom the files belong and the employees of the company; lawyers must take care to choose an appropriate company that has procedures to ensure confidentiality and to admonish the company that confidentiality of the files must be preserved); State Bar of Ariz. Op. 07-02 (2007) (Lawyer may not destroy original client documents after converting them to electronic records without client consent, but may destroy paper documents if they are only copies); State Bar of Cal. Standing Comm. on Prof’l Responsibility & Conduct 2001-157 (2001) (Electronic records may be insufficient if originals are not accurately reproduced, and some documents cannot be copied by law); Fla. Bar Op. 06-1 (2006) (Lawyers may, but are not required to, store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client’s interests; files stored electronically must be readily reproducible and protected from inadvertent modification, degradation or destruction); Me. Bd. of Overseers Op. 185 (2004) (Lawyers may maintain closed files electronically, rather than paper copies, if they are accessible to the client); Me. Bd. of Overseers Op. 183 (2004) (“If an attorney dispenses with the retention of paper files in favor of computerized records, the attorney must be mindful that the obligation to the client may require the attorney to maintain the means to provide copies of those records in a format that will make them accessible to both the attorney and the client in the future. Because the attorney is obligated to ensure that the client is able to make informed decisions regarding the disposition of the file and also must take care in destroying files to be sure that useful information is retained, an attorney will need to consider how new hardware or software will impact future access to old computerized records.”); Mo. Informal Advisory Op. 127 (2009) (Lawyer may keep client’s file in exclusively electronic format except documents that are legally significant as originals and intrinsically valuable documents and providing that the appropriate software to access the information is maintained for the time period the file must be retained); State Bar of Mich. Op. R-5 (1989) (File storage via electronic means should be treated carefully to ensure confidentiality by limiting access to law firm personnel); N.J. Advisory Comm. on Prof’l Ethics Decisions Op. 701 (2006) (Documents may be stored electronically if sufficient safeguards to maintain confidentiality of the documents, particularly if they are stored outside the law firm, except for documents that are client property such as original wills, trusts, deeds, executed contracts, corporate bylaws and minutes); N.Y. County Lawyers Ass’n Op. 725 (1998) (General opinion on the ethical obligation to retain closed files, including that it may be proper for a lawyer to retain only electronic copies of a file if “the evidentiary value of such documents will not be unduly impaired by the method of storage”); N.Y. State Bar Ass’n Comm. on Prof’l Ethics Op. 680 (1996) (Although some items in a client’s file may be stored electronically, some documents (such as original checkbooks, check stubs, cancelled checks, and bank statements) are required by the rules to be kept in original form; documents stored electronically should be stored in “read-only” form so they cannot be inadvertently destroyed or altered; and records must be readily produced when necessary); N.C. State Bar Op. RPC 234 (1996) (Closed client files may be stored electronically as long as the electronic documents can be converted to paper copies, except for “original documents with legal significance, such as wills, contracts, stock certificates, etc.”); S.C. Bar Advisory Op. 02-14 (2002) (General opinion on disposition of closed files when one member of a two-member firm retires, discussing various situations and notes that files may be placed on computer or other electronic media; Note: In South Carolina, the files are the property of the client); S.C. Bar Advisory Op. 98-33 (1998) (The committee declined to give an opinion on electronic retention of closed files as a legal question, but indicated there was no prohibition against retaining documents in electronic format as long as doing so did not adversely affect the client’s interests and as long as the lawyer took reasonable precautions to make sure that third parties with access to the electronic records kept the records confidential); Va. State Bar Op. 1818 (2005) (Lawyer can maintain client files in electronic format with no paper copies as long as the method of record retention does not adversely affect the client’s interests); Wash. State Bar Ass’n Op. 2023 (2003) (Lawyer may have firm file retention policy in which original documents are provided to the client and the lawyer keeps only electronic copies of file materials as long as documents “with intrinsic value” or that are the property of the client cannot be destroyed without client permission); State Bar of Wis. Op. E-00-3 (2000) (If lawyer has stored files electronically, lawyer should provide
F. Solicitation and Advertising

Lawyers may want to offer legal services to persons affected by a disaster. The existence of a disaster, however, does not excuse compliance with lawyer advertising and solicitation rules. Of particular concern is the possibility of improper solicitation in the wake of a disaster. A lawyer may not solicit disaster victims unless the lawyer complies with Model Rules 7.1 through 7.3. “Live person-to-person contact” that is generally prohibited means “in-person, face-to-face, live telephone and other real-time visual or auditory person-to-person communications, where the person is subject to a direct personal encounter without time for reflection,” and a significant motive for the lawyer’s doing so is pecuniary gain. In addition to ethical prohibitions, lawyers should be aware that there may be statutory prohibitions that may apply.

Lawyers may solicit in-person to offer pro bono legal services to disaster victims, because the lawyer’s motive does not involve pecuniary gain. Additionally, lawyers may communicate with disaster victims in “targeted” written or recorded electronic material in compliance with Rules 7.1 through 7.3. Lawyers also should be mindful of any additional requirements for written or recorded electronic solicitations imposed by particular jurisdictions.

---

28 See MODEL RULES OF PROF’L CONDUCT R. 7.1 – 7.5 (all of these Rules were amended in August 2018).
30 MODEL RULES OF PROF’L CONDUCT R. 7.3 cmt. [2] (2018). Rule 7.3(b) contains some exceptions, and Rule 7.3(c) contains an additional prohibition. Both should be consulted.
31 Id.
32 See, e.g., FLA. STAT. §877.02 (Prohibiting solicitation on behalf of lawyers by hospitals, police, tow truck operators, insurance adjusters); 49 U.S.C. §1136(g)(2) (Prohibiting lawyer solicitation within 45 days of an air transportation accident).
33 MODEL RULES OF PROF’L CONDUCT R. 7.3(a); La. Bd. of Ethics Op. 05-RPCC-005 (2005) (Lawyer may solicit disaster victims in person to provide pro bono legal services). Providing pro bono legal services is encouraged by, inter alia, Model Rules 6.1 and 6.2.
34 See, e.g., Rules Regulating the Fla. Bar R. 4-7.18(b)(2) (requiring contrasting “advertisement” mark on envelope and enclosures; statement of qualifications and experience; information on where the lawyer obtained the information prompting the written solicitation; and specified first sentence, among others).
G. Out-Of-State Lawyers Providing Representation to Disaster Victims

Lawyers practicing in jurisdictions unaffected by the disaster who wish to assist by providing legal services to disaster victims must consider rules regulating temporary multijurisdictional practice. Out-of-state lawyers may provide representation to disaster victims in the affected jurisdiction only when permitted by that jurisdiction’s law or rules, or by order of the jurisdiction’s highest court.

The ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster provides that the Supreme Court of the affected jurisdiction must declare a major disaster and issue an order that allows lawyers in good standing from another jurisdiction to temporarily provide pro bono legal services in the affected jurisdiction through a non-profit bar association, pro bono program, legal services program, or other organization designated by the courts. The Model Court Rule also requires those lawyers to register with the courts of the affected jurisdiction, and subjects those lawyers to discipline in the affected jurisdiction.

Conclusion

Lawyers must be prepared to deal with disasters. Foremost among a lawyer’s ethical obligations are those to existing clients, particularly in maintaining communication. Lawyers must also protect documents, funds, and other property the lawyer is holding for clients or third parties.

35 MODEL RULES OF PROF’L CONDUCT R. 5.5 (c), cmt. [14] (2018): “Lawyers desiring to provide pro bono legal services on a temporary basis in a jurisdiction that has been affected by a major disaster, but in which they are not otherwise authorized to practice law, as well as lawyers from the affected jurisdiction who seek to practice law temporarily in another jurisdiction, but in which they are not otherwise authorized to practice law, should consult the Model Court Rule on Provision of Legal Services Following Determination of Major Disaster.” Most states have adopted some form of ABA Model Rule 5.5 on Multijurisdictional Practice. A chart on state implementation of ABA Multijurisdictional Practice Policies compiled by the ABA may be found at: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/recommendations.authcheckdam.pdf.

36 ABA MODEL COURT RULE ON PROVISION OF LEGAL SERVICES FOLLOWING DETERMINATION OF MAJOR DISASTER, available at https://www.americanbar.org/content/dam/aba/images/disaster/model_court_rule.pdf (last visited Sept. 7, 2018). The ABA Chart on State Implementation of ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster can be found at: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/katrina_chart.authcheckdam.pdf.

37 Providing pro bono legal services in this situation would assist the lawyer in meeting the suggested goal of 50 hours per year set forth in Model Rule 6.1(a).

38 As noted above, the Supreme Court of Texas issued an emergency order in 2017 after Hurricane Harvey following the ABA Model Court Order. See supra note 18.
By proper advance preparation and taking advantage of available technology during recovery efforts, lawyers will reduce the risk of violating professional obligations after a disaster.

Dissent: Keith R. Fisher dissents.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

©2018 by the American Bar Association. All rights reserved.
Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer’s confidentiality obligations for e-mail communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: “Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client’s representation.”

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer’s ethical duties.\(^3\)

In 2012 the ABA adopted “technology amendments” to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer’s obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term “cybersecurity” has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of “when,” and not “if.”\(^4\) Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.\(^5\)

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the “technology amendments” made to the Model Rules in 2012, identify some of the technology risks lawyers’ face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”\(^6\) The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

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

---


4. “Cybersecurity” is defined as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI’s Cyber Division, indicated that “[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm’s computer system is a really optimal way to obtain economic and personal security information.” Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

Regarding the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise. The 2012 modification added a new duty in paragraph (c) that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the

---

7. Id. at 43.
8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”
9. MODEL RULES OF PROF’L CONDUCT R. 1.6(a) (2016).
10. Id. at (c).
inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.11

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.12

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- 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).13

11. The 20/20 Commission’s report emphasized that lawyers are not the guarantors of data safety. It wrote: “[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client’s confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances.”

12. ABA CYBERSECURITY HANDBOOK, supra note 3, at 48-49.

13. MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2013). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will
A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client’s information and whether the client’s matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking,
defense or education, may present a higher risk of data theft.\textsuperscript{15} “Reasonable efforts” in higher risk scenarios generally means that greater effort is warranted.

2. **Understand How Client Confidential Information is Transmitted and Where It Is Stored.**

A lawyer should understand how their firm’s electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer’s task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. **Understand and Use Reasonable Electronic Security Measures.**

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As comment [18] makes clear, what is deemed to be “reasonable” may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm’s systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm’s technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider whether certain data should ever be stored in an unencrypted environment, or electronically transmitted at all.


Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client’s lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party. If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or

---


17. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One’s Client (2011). Formal Op. 11-459 was decided before the 2012 change to Rule 1.6. Those changes, adding 1.6(c), now says that lawyers “shall” make reasonable efforts to prevent the unauthorized or inadvertent access to client information. See, e.g., Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer’s email server).
receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.\textsuperscript{18}

5. **Label Client Confidential Information.**

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.\textsuperscript{19}

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

6. **Train Lawyers and Nonlawyer Assistants in Technology and Information Security.**

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably

\textsuperscript{18} Some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, \textit{e.g.,} Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:
- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- 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…;
- 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;
- 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
- 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.

\textsuperscript{19} See Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).
assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.20

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client

information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”21 If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.22

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.23 The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to

---

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2017). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, “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.”

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(e) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.
Opinion #220. Cyberattack and Data Breach: The Ethics of Prevention and Response

Issued by the Professional Ethics Commission

Date Issued: April 11, 2019

The American Bar Association issued Formal Opinion No. 483 on October 17, 2018, addressing a lawyer’s obligations after suffering an electronic data breach or a cyberattack. The Professional Ethics Commission wanted to take this opportunity to recommend the ABA’s Opinion to the Maine Bar and to address a Maine lawyer’s obligations under the Maine Rules of Professional Conduct both before and after a data breach or cyberattack has occurred.

**Question:** What are a lawyer’s ethical obligations to understand the risks posed by technology, to prevent a cyberattack or data breach, and to respond once one occurs?

**Short Answer:** A lawyer’s professional obligations, of course, are not limited merely to the practice of law. Any lawyer who chooses to use technology in order to provide legal services for clients has an obligation to make sure that technology is serving the clients and not disserving them. That obligation applies both before and after a third party uses the lawyer's technology for their own gains or for other purposes contrary to the interests of the lawyer’s clients. The overriding obligation is to know what the technology does, what it does not, and how to use it safely. If, despite the lawyer’s reasonable efforts to protect electronic data created and stored in the service of clients, a third party defeats those efforts, the lawyer’s obligations are to take reasonable action in order to stop or contain the attack or breach; to investigate and ascertain whether confidential information relating to clients has been, or may have been, compromised; to determine whether the representation of current clients has been, or may have been, significantly impacted or impaired; and to promptly notify current and former clients.

**Rules Implicated:**

- M.R. Prof. Conduct 1.1 - Competence
- M.R. Prof. Conduct 1.3 - Diligence
M.R. Prof. Conduct 1.4 - Communications with Clients
M.R. Prof. Conduct 1.6 - Confidentiality of Information
M.R. Prof. Conduct 1.9 - Duties to Former Clients
M.R. Prof. Conduct 1.15 - Safekeeping Property
M.R. Prof. Conduct 5.1 - Responsibilities of Partners, Managers, Supervisors
M.R. Prof. Conduct 5.3 - Responsibilities regarding Non-Lawyer Assistance

Since this Opinion cannot cover every ethical obligation associated with the expanding role of technology in everyday legal practice, the Commission recommends further reading to include not only the resources cited in this Opinion, but also Commission Opinions No. 207 (“The Ethics of Cloud Computing and Storage”), No. 196 (“The Transmission, Retrieval and Use of Metadata Embedded in Documents”), and No. 195 (“Client Confidences: Communications with clients by unencrypted e-mail”).

**PROFESSIONAL DUTIES: PREVENTION**

**Discussion:** In the case of a data breach or cyberattack, the standard for measuring ethical conduct is not one of strict liability, but reasonableness. The Commission agrees with the ABA Standing Committee on Ethics and Professional Responsibility that the standard of care “does not require the lawyer to be invulnerable or impenetrable. Rather, the obligation is one of reasonable efforts.” ABA Formal Opinion No. 483 at p. 9. Efforts that are deemed to be reasonable, furthermore, do not fit into a neat formula, but are measured based on “a fact-specific approach to business security obligations that requires a ‘process’ to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.” JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS, 124 note 11, at p. 73 (2d ed. 2018).

 Appropriately, the first Rule of Professional Responsibility is that of competence. “A lawyer shall provide competent representation to a client.” M.R. Prof. Conduct 1.1. While the Rule goes on to talk about “legal knowledge, skill, thoroughness, and preparation,” the lawyer’s obligation of competence extends beyond the “legal” and into the technological, if the lawyer relies on technology to provide legal services.

The Comments to Rule 1.1 mention that competent handling of a matter involves an analysis not only of the factual and legal elements of the problem, but also of the “methods and procedures meeting the standards of competent practitioners.” M.R. Prof. Conduct 1.1 cmt. (5). Those methods and procedures often include using technology to communicate with clients, to store documents and information, to research the facts, to evaluate documentary evidence, and to produce documents, all of which activities introduce the risk
of unauthorized access by third parties. “The required attention and preparation are determined in part by what is at stake....” *Id.*. The more confidential, sensitive, or valuable the client’s data, the greater the risk of harm to the client if a third party accesses them, and the more attention needs to be paid to the technology employed in representing the client.

Attending to the methods and procedures used to represent a client means that “a lawyer should keep abreast of changes” not only in the law, but also in “its practice.” *Id.*, cmt. (6). Keeping abreast of practice changes means seeking education on evolving technology on a regular basis in order to maintain competence in its use. Id. M.R. Prof. Conduct 1.3 similarly requires that a lawyer shall “act with reasonable diligence and promptness in representing a client,” including using technology in the course of representing the client. A lawyer who lacks individual competence to evaluate and employ safeguards to protect client confidences and secrets should seek education from an expert or associate with another lawyer who is competent. See ABA Formal Opinion 477R (May 11, 2017, revised May 22, 2017).

ABA Formal Opinion No. 483 summarizes the lawyer’s responsibility succinctly in noting that the ABA’s counterpart to Maine’s Rule 1.1 requires “lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer’s competency in this regard may be satisfied either through the lawyer’s own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.” ABA Formal Opinion No. 483 at p. 4. However, the Commission does not mean to suggest that it endorses a complete ignorance of technology just because an associated lawyer or staff member knows all about it. A baseline understanding of, and competence in, the technology used in the practice of law must be maintained by every lawyer.

Where the duty competence in technology intersects with the duty to protect the confidentiality of a client’s information, M.R. Prof. Conduct 1.6 becomes relevant to the discussion. “A lawyer shall not reveal a confidence or secret of a client” except under enumerated circumstances typically involving the client’s consent. A “confidence” means information protected by the attorney-client privilege. A “secret” means information, not privileged, that relates to the representation and for which “there is a reasonable prospect that revealing information will adversely affect a material interest of the client” or information that the client has instructed the lawyer not to reveal. There is no client consent to reveal confidences or secrets to a third party who accessed that information without authorization using technology. Consequently, Rule 1.6 may be violated when an electronic data breach or cyberattack occurs and the lawyer did not “act competently to safeguard information relating to the representation against inadvertent unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or are
subject to the lawyer’s supervision.” M.R. Prof. Conduct 1.6 cmt. (16).

Of course, the lawyer’s duty to prevent unauthorized access also applies to electronic communications. “When transmitting a communication that includes confidences or secrets of a client, the lawyer must take reasonable precautions to prevent the information from coming to the hands of unintended recipients.” Id., cmt. (17). The ABA’s Formal Opinion No. 477R provides a comprehensive discussion of the ethical responsibility incumbent on a lawyer when communicating with a client using the Internet. “A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.” ABA Formal Opinion No. 477R at p. 1. Maine’s Rule 1.6 “does not require that the lawyer use special security measures if the method of communicating affords a reasonable expectation of privacy. Special circumstances, however, warrant special precautions.” M.R. Prof. Conduct 1.6 cmt. (17). The extent to which a communication is protected by law or by a confidentiality agreement are two factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality and privacy. The sensitivity of the information and its impact on the client, should it fall into wrong hands, is another factor.

Of course, the client’s wishes must be followed when it comes to security. “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 the means of communication that would otherwise be prohibited by this Rule.” Id. In the case of less protection than Rule 1.6 may require, the informed consent discussion the lawyer has with the client should be thorough and documented. The issue of what constitutes sufficient informed consent is different from client to client and from situation to situation. The Commission recommends that a lawyer who seeks to obtain a client’s consent to less protection than the Rules may require consult court and other decisions addressing whether discussions precipitating client consent were sufficient in other instances.

Lawyers should be well-versed in the fact that electronic data can constitute “property” of the client for which Rule 1.15 requires a duty of safekeeping. The duty lawyers owe to protect hardcopy documents and other tangible property given to them by clients applies equally to electronic data. Even when the representation has ended, the lawyer has an obligation to “retain and safeguard such information and data for a minimum of eight (8) years” or longer if the data has intrinsic value. M.R. Prof. Conduct 1.15(f). Generally speaking, “a lawyer should hold property of others with the care required of a professional fiduciary,” M.R. Prof. Conduct 1.15 cmt. (1), and that includes electronic data. The Rules
extend this fiduciary responsibility beyond the lawyer who is working individually with the client. It includes that lawyer’s partners and any attorney who exercises “comparable managerial or authority in the law firm.” M.R. Prof. Conduct 5.1(a) & (c)(2). The Rules “impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct.” ABA Formal Opinion No. 483 at p. 4. See, also, M.R. Prof. Conduct 5.1(a).

A lawyer’s responsibility for non-partners who are not diligent in their understanding and use of technology is limited to situations where the lawyer ordered or ratified the conduct with knowledge of it. M.R. Prof. Conduct 5.1(c)(1). When a lawyer has direct supervisory authority over another lawyer, on the other hand, they must “make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.” M.R. Prof. Conduct 5.1(b). The supervising attorney can be responsible for the other attorney’s non-conformance with the Rules if the attorney “knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.” M.R. Prof. Conduct 5.1(c)(2).

Individual attorneys are not absolved of their ethical duty to abide by the Rules of Professional Conduct by virtue of the fact that another partner, member of management, or other attorney has assumed greater duties with respect to certain requirements of the Rules. It is a violation of Rule 5.1 if an attorney knows precious little about the risk technology poses to a client, uses that technology, and causes the inadvertent revelation of the client’s confidences or secrets, even if another attorney in the firm is the foremost expert in the technology. M.R. Prof. Conduct 5.1 cmt. (8); M.R. Prof. Conduct 5.2(a). It is not enough to rely on another attorney in a firm who is fluent in the current state of technology and its risks, limitations, and benefits. All partners, shareholders, and other members of a professional organization of lawyers, in addition to the management designated by those organizations, have an obligation to ensure that there are sufficient internal policies and procedures for conformance with the Rules of Professional Conduct.

Lawyers who are partners, management, and direct supervisors in a law firm have a duty with respect to their non-lawyer staff too. M.R. Prof. Conduct 5.3. Support staff, even if independent contractors, must be given “appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose the information relating to representation of the client, and should be responsible for their work product.” M.R. Prof. Conduct 5.3 cmt. (1).

In addition to training lawyers and staff, the Commission agrees with the ABA that “based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, lawyers must employ reasonable efforts to monitor the technology and office resources
connected to the internet, external data sources, and external vendors providing services relating to data and the use of data.” ABA Formal Opinion No. 483 at p. 5. The responsibility is two-fold: (1) supervising the use of technology by lawyers and staff to ensure it is consistent with their training and instruction, and (2) monitoring the status of the technology itself in order to reveal attacks and breaches as soon as reasonably detectible.

PROFESSIONAL DUTIES: RESPONSE

In Opinion No. 207, the Commission noted that “[w]hat changes with evolving technology is not the overriding ethical constraints on counsel, but how those constraints are satisfied with respect to new challenges presented by that technology.” The ABA has observed that fulfilling a lawyer’s responsibilities after a data breach or cyberattack requires the lawyer to “understand technologies that are being used to deliver legal services to their clients” in the first place. ABA Formal Opinion No. 483 at p. 4. Once the duty to understand the technology being used has been met, the lawyer’s corollary duty involves how to address a problem with that technology when it arises. The Commission recommends creating a plan to address known or suspected security breaches, including the identification of persons to be notified, in order to assist counsel with their ethical obligations.

If no confidential information relating to a client has been, or may have been, compromised, and the representation of a client has not been significantly impacted or impaired by the cyberattack or data breach, the lawyer’s ethical obligation may be limited to making reasonable efforts to prevent a reoccurrence. For example, the lawyer or the law firm may need to install or update security systems or technology or seek additional training. If the lawyer has an obligation to notify clients at all, it may be limited to the dictates of federal or state law. See, e.g., 10 M.R.S. §§ 1346-1350B (notice of risk to personal data); 45 C.F.R. §§ 164.404-414 (HIPAA breach notification rules); 15 U.S.C. §§ 6801, et seq. (disclosure of nonpublic personal information requirements under the Graham-Leach-Bliley Act).

Notification requirements under the Maine Rules of Professional Conduct arise when confidences or secrets are exposed or the breach significantly impairs or impacts the representation of a client. A cyberattack or data breach alone may give rise to a duty to notify clients, depending on the circumstances. Rule 1.3 requires that the lawyer “act with reasonable diligence and promptness in representing a client.” Rule 1.4 provides that the lawyer “keep the client reasonably informed about the status of the matter.” Once the scope of an attack or breach is understood, the lawyer must promptly and accurately make an appropriate disclosure to the client. We agree with the ABA that the Rules “do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means.” ABA Formal Opinion No. 483 at p. 7.
Due to the nature and scope of the cyberattack or data breach, the lawyer may reasonably believe that, in addition to the client, a disclosure should be made to third parties. Disclosure to third parties revealing confidential client information requires an analysis under Rule 1.6 to determine whether informed consent must first be obtained from the client or whether one of the exceptions applies. For example, the lawyer may make a disclosure to law enforcement with or without the informed consent of the client if the lawyer must make the disclosure in order to comply with applicable law. “Although the public interest is usually served by a strict rule requiring lawyers to preserve the confidentiality of confidences and secrets of clients’ information,” M.R. Prof. Conduct 1.6 cmt. (6), that rule is not without its exceptions. It is conceivable that a cyberattack or data breach could expose confidential information that presents a risk to public safety. Under those circumstances, a lawyer may disclose confidential information in order to prevent reasonably certain substantial bodily harm or death.

While the Commission agrees with the analysis contained in ABA Formal Opinion No. 483 concerning notification of a current client, the Commission departs from the ABA with respect to a former client. The ABA reviewed Model Rules 1.9 and 1.16 and concluded that notice to a former client is not required. However, Maine’s Rule 1.9 provides that a “lawyer who has formerly represented a client shall not thereafter: (2) reveal confidences or secrets of a former client except as these Rules would permit or require with respect to a client.” The duty of confidentiality survives the termination of the client-lawyer relationship. M.R. Prof. Conduct 1.6 cmt. (18). Indeed, trust is the “hallmark of the client-lawyer relationship,” id., cmt. (2), whether for a current or a former client. The Commission concludes that a former client is entitled to no less protection and candor than a current client in the case of compromised secrets and confidences. A former client must be timely notified regarding a cyberattack or data breach that has, or may have, exposed the client’s confidences or secrets.

In addition, Rule 1.15(f) requires that “upon termination of representation, a lawyer shall return to the client or retain and safeguard in a retrievable format all information and data in the lawyer’s possession to which the client is entitled.” (Emphasis added.) The Commission recently issued an Enduring Ethics Opinion commenting on Commission Opinion No. 187 and clarifying that information and data is entrusted to the attorney for safekeeping for both current and former clients.

Finally, as previously noted in the prevention of cyberattacks or data breaches, M.R. Prof. Conduct Rules 5.1 and 5.3 require a lawyer to take reasonable measures to provide assurance that the conduct of lawyers and non-lawyer assistants in a law firm is compatible with the professional obligations of the lawyer. The ethical obligations of a lawyer that arise after a cyberattack or data breach, including taking reasonable actions to stop or contain it, investigating the attack or breach, and notifying affected current and former clients are
shared by many in the law firm.

### Enduring Ethics Opinion

**Credits**

Copyright © 2013
All rights reserved.