CYBERSECURITY: ETHICAL AND PRACTICAL CONSIDERATIONS

Presented by:

Craig A. Bramley, Esq.
Berman & Simmons PA, Lewiston

Benjamin W. Lund, Esq.
Brann & Isaacson, Lewiston

Suzanne E. Thompson, Esq.
Board of Overseers of the Bar, Augusta

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.

Question

May Maine attorneys and firms use third party vendors to store confidential client information electronically? May cloud-based software be used to store and transmit client information?

Short Answer

Yes. Attorneys and firms may use third party vendors and cloud-based software to store and transmit client information. However, to comply with their duties of competence, diligence, and confidentiality, attorneys and firms must screen third party vendors to ensure they understand how vendors and products work and to confirm that the vendors and software will adequately protect client information and firm data.

Applicable Rules

- Rule 1.1 Competence
- Rule 1.3 Diligence
- Rule 1.6 Confidentiality of Information
- Rule 1.9 Duties to Former Clients
- Rule 1.15 (safeguarding client property)
- Rule 1.18 Duties to Prospective Clients
- Rule 5.3 (supervision of third parties)

Discussion

Technology has a substantial influence over lawyers' and law firms' practice of law. Technological advances can expand the quality of services provided by lawyers and save time, but it is important to consider the implications of new technology as it relates to lawyers' ethical duties under the Rules of Professional Conduct. Third party vendors can be used for various aspects of law practices like routine office work and transcription. However, over the past decade, technological advances in electronic communication and data storage have given lawyers many options to store and transmit data through third-party vendors including but not limited to: data storage, document sharing, case management systems, email, phone/voice communication, voice messaging, standard messaging systems, banking and other financial management systems, and various website applications that may be used on firm sites including forms and the use of artificial intelligence in triaging potential clients. In fact, Rule 31(B)(3) of the Maine Rules of Electronic Court Systems requires lawyers to have an email address, which nearly always involves the use of a third-party vendor. Many of these third-party vendor services also involve the use of cloud storage vendors like Microsoft and Amazon which can mean there are multiple layers of third-party vendors involved in a single application. It is nearly certain that technological advances will continue to develop so that practitioners reading this opinion in years to come will have much longer lists of technological third-party vendors in use. This opinion should be read to apply to all third-party vendors, including technology vendors, cloud-based systems, and whatever next generation technology systems become available in the future.

While technology and third-party vendors can enhance and improve the quality of services lawyers provide clients, there are several ways in which the Rules of Professional Conduct are implicated by the use of third-party vendors, including: competence, diligence, client confidentiality, secured storage of client files, and supervision of nonlawyers. The Commission affirms previous opinions that found that lawyers are permitted to use third-party vendors including technology vendors and vendors utilizing cloud-based storage, as long as lawyers conduct thorough risk assessments before engaging with a third-party vendor and throughout a third-party vendor relationship. The Commission issues this Enduring Ethics Opinion to consolidate previous Opinions touching upon these issues and to clarify the broad applicability of these standards to a wide range of technology and vendors.

A. History of Commission Opinions

The Professional Ethics Commission has addressed the ethical implications of storing and transmitting client information electronically in several opinions. In 2004, the Commission first provided guidance around the storage of client files in Opinion #183. Four years later, Opinion #194 addressed the ethical implications of using third-party vendors to store client data and provided a framework of factors lawyers should consider when contracting with third-party vendors. Cloud computing was first addressed in Enduring Ethics Opinion #194[1] which was intended to clarify that Opinion #194 is applicable to cloud storage vendors. To further clarify, Opinion #207 was issued in 2013 and more specifically addressed the ethical implications of the use of cloud-based storage.

B. Applicability of Rules

Client confidentiality as laid out by Rule 1.6 is the cornerstone of the attorney-client relationship and prohibits a lawyer from sharing confidential client information, privileged information, and client secrets with third parties. The duty of confidentiality extends after the attorney-client relationship has ended in Rule 1.9 and to prospective clients in Rule 1.18. Using outside vendors to store and transmit data in any form means a lawyer is giving access to client information to the technicians and employees of the vendor. Additionally, the use of electronic and cloud-based storage creates cyber security risks that threaten client confidentiality. A 2020 survey of law firms by the ABA found that 29% of firms had experienced a cyber security breach in the preceding 12 months.[2]

Technological advances do not change lawyers' obligations to their clients. Other Commission opinions discuss the nuances of the confidentiality rules at length. For the purpose of this opinion, it is important to note that the portions of client information that are owed a duty of confidentiality must be protected when accessible to, stored by, or transmitted through third-

[1] This same Enduring Ethics Opinion also updated Opinion #183 and stated that the obligations under the former Bar Rules carried over to the Rules of Professional Conduct and included an obligation to retain and safeguard client records that have "intrinsic value in the particular version, such as original signed documents."

[2] ABA Tech Report 2020, https://www.lawtechnologytoday.org/2020/10/techreport-2020-cybersecurity/?utm_medium=email&utm_source=salesforce_303064&sc_sid=03660239&utm_campaign=YOURABA&promo=YOURABA&utm_content=&additional4=&additional5=&sfmc_j=303064&sfmc_s=45074674&sfmc_l=2776&sfmc_jb=26&sfmc_mid=100027443&sfmc_u=9012336.

party vendors. Further, lawyers have an obligation to securely store client information for a minimum of 8 years after the conclusion of an attorney-client relationship under Rule 1.15(f).

Rules 1.1 and 1.3 provide that lawyers have general duties of competence and diligence in their work. These duties include understanding how technology works and how to use technology safely and securely. Lawyers should make sure to understand how to securely use the technology they purchase and incorporate into their law practices including understanding what third-party access is involved, who might have access to it, and what level of security the application uses. It is also important for lawyers to understand where and how information is stored. Many forms of electronic communication result in unintended storage of client information through features like chat histories and lawyers must be careful to avoid cyber security risks.

Lawyers can rely on the expertise of internal nonlawyer employees and third-party vendors to ensure the use of safe and secure technology but lawyers must remain mindful that they bear the ultimate responsibility for the protection of client data under the Rules. Lawyers have a duty to supervise nonlawyers with access to client data under Rule 5.3. Rule 5.3 includes a duty to ensure the nonlawyer's conduct is compatible with the ethical obligations of the lawyer and makes the lawyer responsible for the conduct of nonlawyers that violates the Rules of Professional Conduct when the lawyer orders the conduct or, in the case of a partner or comparable manager, knows of the conduct. This supervision is straightforward for in-house technology staff. However, the duty is also applicable to third-party vendors. While lawyers cannot supervise the day-to-day work of third-party vendors, lawyers must supervise the vendor relationship by conducting the appropriate risk assessment before contracting with third party vendors. Lawyers must ensure that engaging with a third-party vendor does not put client information at risk. Lawyers should be aware that failure to properly vet the practices and security of third-party vendors could make them liable for ethics rule violations that occur because of the vendors' actions or failure to act.

In addition to ethics rules, there are numerous state and federal laws that create requirements for the secure storage and confidentiality of specific types of information. Lawyers should familiarize themselves with the requirements that apply to their practices, stay informed of any changes or updates to such requirements, and ensure compliance.

C. Screening Vendors.

Screening vendors is not a unique best practice for lawyers. Vendors should be accustomed to answering questions about their practices and security. Some may have answers to standard due diligence questions available. Lawyers should consider adopting their own due diligence questions to use for routine screening of potential and current vendors. Contracts with vendors should be carefully reviewed to ensure there are adequate protections to protect client information and comply with the Rules.

As part of their due diligence in assessing technology vendors, lawyers should make use of available resources in developing screening questions and analyzing contracts for technology vendors. Lawyers should be aware of best practices and industry standards and stay up to date on the recommendation of experts. Some examples of standards to consider in assessing a vendor

include the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the American Bar Association (ABA) Cybersecurity Legal Task Force's *Vendor Contracting Project: Cybersecurity Checklist, Second Edition (2021).*

There are a variety of screening questions and assessments that would meet a lawyer's duty of due diligence. The following is a list of suggested topics for assessment:

- The risks created by using the vendor.
- Where the data is hosted and how local laws in the relevant jurisdiction affect the security of the data.
- Recent security breaches and incidents.
- Pending or threatened regulatory actions against the vendor.
- Licenses and certificates held by the vendor.
- Qualifications of the vendor's employees.
- The vendor's overall information security program, including regular monitoring, testing, and maintenance. Close attention should be paid to the vendor's encryption, back up policies, and audits, all of which should be freely available to the lawyer or law firm.
- The vendor's incident management protocols, including reporting to customers and business continuity plans.
- The vendor's insurance and any liability or indemnification contract provisions.
- How the vendor defines the scope of its responsibilities.
- Confidentiality procedures and policies at the vendor.
- Who will have access to client and firm information, how it will be accessed, and how access will be tracked.
- Whether using the vendor involves any additional third-party vendors.
- The vendor has the rights to products, software, and data held by the vendor.
- The lawyer or law firm's continued sole ownership of data and prohibitions on the use of the data by vendor for other purposes.
- The process for terminating the relationship and the vendor's obligation to return or destroy data and information.

Lawyers should be cautious of vendors that do not provide opportunities for questions or assessment. For example, mass market social media applications generally would not allow a lawyer to negotiate security policies. These applications would be insecure to use to store or transfer confidential client information if they do not allow a lawyer or law firm adequate control over its data.

Once vendors and software are selected, lawyers and firms must continue to pay attention to on-going cyber security risks. Lawyers and firms must be prepared to respond to a cyber security breach and can seek guidance in Opinion #220. Lawyers must also consider how their day-to-day operations implicate cyber security risks, for example, there is guidance on the use of email to communicate with clients in Opinion #195. Cyber security risks also exist internally at law firms. Lawyers should diligently ensure that internal controls are in place to protect the firm from cyber

security threats. This includes making sure the firm has a proper back up system, firewalls, and protocols for disclosure of information and information access. Law firms should also educate and train employees on cyber security risks.

The efficient and effective modern practice of law involves the use of technology. There are inherent cybersecurity risks that come with the use of third party vendors that implicate lawyers' ethical obligations. It is not possible for lawyers or law firms to seek risk-free technology vendors. Instead, lawyers must weigh the benefits, risks, and protections of a particular vendor and seek to protect client information to the best of their ability. Lawyers should maintain a standard of due diligence in assessing and monitoring vendors that allows lawyers and law firms to keep up with evolving best practices for both security and the efficient practice of law.

NOTES