ALFA International
The Global Legal Network
Celebrating 40 Years

PROTECTING YOUR FIRM'S DATA WHILE PERMITTING REMOTE WORK: TECHNOLOGICAL COMPETENCE AND ETHICAL REQUIREMENTS

AUTHORED BY ALFA INTERNATIONAL ATTORNEYS:

Devin J. Chwastyk
MCNEES WALLACE & NURICK LLC
Harrisburg, PA
dchwastyk@mcneeslaw.com

Leslie Whitten
YOUNG CLEMENT RIVERS, LLP
Charleston, SC
lwhitten@ycrlaw.com

Shannon "A.J." Singleton
STOLL KEENON OGDEN, PLLC
Lexington, KY
aj.singleton@skofirm.com

PROTECTING YOUR FIRM'S DATA WHILE PERMITTING REMOTE WORK: TECHNOLOGICAL COMPETENCE AND ETHICAL REQUIREMENTS

The Ethical Requirements for Technological Competence

The American Bar Association ("ABA") Model Rules of Professional Conduct (and corresponding state rules) make clear the obligation on attorneys to take necessary measures to protect client data. The ABA has also released opinions related to protecting data, as well as specific obligations during a cyber-event.

Model Rule 1.1 indicates 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." Pursuant to Model Rule 1.1, comment 8, attorneys are also required to stay abreast of the "risks associated with relevant technology" in order to competently represent their clients.

Model Rule 1.6(a) prohibits an attorney from revealing "information relating to the representation of a client unless the client gives informed consent [and] the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)." Moreover, Model Rule 1.6(c) requires 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."

To further explain Model Rule 1.6(c), Comments 18 and 19 of the Rule regarding "Acting Competently to Preserve Confidentiality" state:

> [18] 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. 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. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

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

Model Rule 1.9 generally prevents attorneys from revealing information on former clients related to the representation, and Model Rule 1.15 requires attorneys to appropriately hold and safeguard client information or property. Several state ethics decisions make clear that client files, and therefore data provided by clients to their lawyer, are encompassed in the definition of "client property."

Under Model Rule 5.1, attorneys have a duty to make a reasonable effort to ensure that attorneys they supervise comply with the Rules of Professional Conduct. Similarly, under Model Rule 5.3, an attorney having supervisory authority over non-lawyer employees has an ethical duty to take reasonable steps to ensure that the non-lawyer's conduct is consistent with an attorney's professional obligations under the Rules of Professional Conduct.

Law firm employees and staff also have a duty to securely maintain electronically-stored client information. ABA Resolution 109 recognizes that "[l]awyers and law offices have a responsibility to protect confidential records from unauthorized access and disclosure, whether malicious or unintentional, by both insiders and hackers." Law firms and other organizations must "develop, implement, and maintain an appropriate cybersecurity program" addressing security controls and requiring regular testing and assessments.

ABA RESOURCES AND OPINIONS

As a resource for practitioners, the ABA also has published its Cybersecurity Handbook, which addresses methods by which lawyers and law firms can implement appropriate data security measures. In light of these ethics rules, law firms face particular hazards from data breaches, even beyond the "routine" and tremendous liability risks confronted by private companies that collect and maintain databases of personally-identifiable information. While private companies may face private claims or enforcement actions for violations of state and federal privacy laws, law firms face the added risk that any negligence on their part leading to the exposure of client data could be found to constitute legal malpractice and violations of state ethics rules, potentially leading to attorney disciplinary proceedings.

In the last three years, the ABA has issued ethics opinions addressing the lawyer's (and, by extension, the law firm's) duties with respect to Model Rule 1.6(c) for implementing technological safeguards to protect the confidentiality of information relating to the representation of a client. Most notably, ABA Formal Opinion 477R (revised May 22, 2017) ("Securing Communication of Protected Client Information") addresses the lawyer's ethical obligations under Rule 1.6(c) and the changing technological environment.

ABA Formal Op. 477R starts with the sobering recognition that the world is very different from when the ABA issued Formal Op. 99-413 in 1999, in which the ABA opined:

> Lawyers have a reasonable expectation of privacy in communications made by all forms of email, including unencrypted email 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.

See ABA Formal Op. 477R, at p. 1, citing ABA Formal Op. 99-413, at p. 11.

In re-evaluating its position, the ABA states in Formal Op. 477R:

> Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when" and not "if." 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 the hacker and likely less voluminous than that held by the client.
>
> However, cyber-threats and the proliferation of electronic devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email.

See ABA Formal Op. 477R., at pp. 2 and 5. As such, the ABA opines in Formal Op. 477R:

> A lawyer generally may transmit information relating to the representation to 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 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 high degree of security.

See ABA Formal Op. 477R, at p. 1.

To comply with this Rule 1.6 duty of confidentiality, ABA Formal Op. 477R provides the following guidance: (1) understand the nature of the threat; (2) understand how client confidential information is transmitted and where it is stored; (3) understand and use reasonable electronic security measures; (4) determine how electronic communications about a client's matters should be protected; (5) label client confidential information; (6) train lawyers and non-lawyer assistants in technology and information security; and (7) conduct due diligence on vendors providing communications technology. See ABA Formal Op. 477R, at pp. 6-10.

The ABA has also addressed, in ABA Formal Op. 483 (Oct. 17, 2018), the "Lawyer's Obligations After an Electronic Data Breach or Cyberattack." The Opinion summarizes its findings by explaining:

> 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 the clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

See ABA Formal Op. 483, at p. 1.

Lawyers have an ethical duty to monitor for a data breach, i.e., incidents in which material client confidential information has been or is likely to have been lost, compromised, or misappropriated. But the ABA also recognizes that lawyers are not generally cyber security experts; therefore, it is appropriate for lawyers to employ or retain technology experts to help monitor for breaches.

Lawyers also have an ethical responsibility to make reasonable efforts to establish security-related policies and procedures and to train themselves and their staff members on such matters. The Opinion explains: "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." *Id*., at p. 6.

If the lawyer does learn that he/she is the victim of a data breach, the lawyer must act promptly to stop the breach and mitigate the damage. Reasonable efforts, in this regard, would likely include having already in place and then implementing an "incident response plan." The Opinion explains:

> 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 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.

Id., at p. 6-7, *quoting* Steven M. Puiszis, Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning, The Professional Lawyer, Vol. 24, No. 3 (Nov. 2017). And if the lawyer is the victim of an attack, he/she should also do what he/she can, either him/herself or through outside consultants, to restore operations and retrieve data.

After taking reasonable steps to mitigate the damage, the competent lawyer will thereafter attempt to (a) determine how the breach occurred, which may assist in assessing what information was lost or compromised, and (b) take steps to prevent similar breaches in the future.

At the heart of ABA Formal Op. 483 is the Opinion's discussion of the lawyer's obligations to provide notice of the data breach to clients. With respect to current clients, the Opinion notes that Model Rule 1.4(b) requires the lawyer to explain to the client anything "reasonably necessary" for the client to make informed decisions about the representation. Because of the requirements imposed by Model Rule 1.4, the lawyer has an obligation to

notify the client about a data breach: "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 probability of being negatively impacted." ABA Formal Op. 483, a p. 11. However, with respect to former clients, the ABA Standing Committee took a different approach. It was unwilling to impose an ethical obligation to notify former clients in the absence of a written rule requiring such notification as a matter of legal ethics. *Id*., at p. 13.

Best Practices for Technological Competence

Law firms collect and maintain a wealth of confidential data, yet many have only relatively recently begun to truly internalize their obligations to protect the security of that information. The data maintained by law firms in their files often includes information likely to be targeted by hackers, including trade secrets, intellectual property, information concerning confidential transactions, and client's intimate personal information. Meanwhile, as a practical matter, implementing data security measures in law firms can be especially difficult due to the nature of legal work and the reluctance of attorneys to complicate their work or inconvenience clients with encryption or other proactive steps.

There is no regulation or direct guidance as to the appropriate standard of care that should be adopted, or specific steps that law firms should take, to secure client data. However, it is becoming an industry standard for law firms to have an "organization-wide security program." The recommended elements for such a program will vary widely among law firms depending on their size, type of practice, base of clients, and use of technology. In any case, law firms must internalize and adopt the same sort of advice for a client seeking to prevent unauthorized access to its information and to protect itself from liability should any such access occur. With that in mind, a law firm's "organization-wide security program" certainly should include the following elements:

A. A written information security policy, disseminated to all attorneys and employees upon hiring and annually thereafter, with required acknowledgment of receipt and defined disciplinary steps for violations;
B. Annual training of attorneys and employees with regard to the importance of data security and implementation of the information security policy;
C. Classification of data stored by the firm by degree of confidentiality and access controls limiting attorneys and employees from viewing or downloading data not within their level of access or necessary purview;
D. A data breach response plan, designating the responsible persons within the firm to be notified of any potential breach, identifying pre-screened IT vendors and outside counsel to assist in the response, and outlining the requisite steps to be followed by the team, including: remediation of the breach; identification of affected records; and notification in accordance with applicable state laws to clients and other individuals whose personally-identifiable information was included in those records;
E. Third-party outside audits by independent vendors conducting risk assessments, security audits, and penetration testing on some regular basis (frequency determined by the degree of risk created by the nature of the firm's practices, clients, and operations);
F. Record retention policies that limit the amount and type of electronic and paper records maintained by the firm and providing for destruction and deletion of those records on a schedule in line with industry standards and applicable ethical rules;
G. Mandatory use of a virtual private network or similar utility for remote access to the firm's network and requirements for encryption of documents transferred to any removable media, laptop, smartphone, or other device, so that files are not accessible from any such device lost or stolen;

H. Other appropriate technological tools for the shutoff of remote access, allowing the disabling or deletion of devices remotely, and requiring regular changing of mandatory complex passwords for access to the firm's network;
I. Controls on physical access to the firm's offices, storage facilities, file rooms, and filing cabinets to prevent the theft or loss of paper files and third-party access to computer hardware on-site;
J. Policies for vendor access to the firm's network and physical locations, along with indemnification language in contracts with vendors allocating the risk for a data breach resulting from any intentional or negligent acts by the vendor's employees;
K. Due diligence in the selection and use of cloud-computing vendors to store and maintain confidential documents to ensure the vendor has adequate safeguards in place to protect that data (see, e.g. Pa. Bar Association Formal Opinion 2011-200: "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."); and
L. Appropriate cyber-insurance in addition to or as an endorsement to legal malpractice and general liability policies.

Cybersecurity is a constantly changing area that affects all of us on a daily basis. While there is a sense of apathy among those outside of the arena, attorneys have an ethical responsibility to take reasonable steps to ensure that client information is adequately protected from inadvertent or unauthorized disclosure, or unauthorized access. Proper communication among attorneys and employees, and between attorneys and their clients, along with understanding the risks, is essential for all computer users. However, attorneys have a unique responsibility under the applicable ethics rules.