2023 New York Statewide Civil Legal Aid Technology Conference

2A Agents of the SHIELD - Data Privacy and Security
Wednesday, April 19, 2023
1:00 PM – 1:50 PM
Live Virtual Presentation
CLE Credits: 1.0 Cybersecurity, Privacy and Data-Ethics

CLE Resources

Stop Hacks and Improve Electronic Data Security Act ("Shield Act")

NY State Senate Bill S5575

New York Rules of Professional Conduct 1.1, 1.4, 1.6, 5.1, 5.2, 5.3

ABA Formal Opinion 477R: Securing Communication of Protected Client Information

ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach of Cyberattack

ABA Formal Opinion 498: Virtual Practice

NYSBA Ethics Opinion 1240: Duty to Protect Client Information Stored on a Lawyer's Smartphone

NYSBA Ethics Opinion 1019: Confidentiality; Remote Access to Firm's Electronic Files

NYSBA Ethics Opinion 842: Using an Outside Storage Provider to Store Client Confidential Information

New York State Continuing Legal Education Requirements: Cybersecurity, Privacy and Data Protection FAQs

Supplemental Materials

Agents of the SHIELD - Data Privacy and Security | Cybersecurity, Privacy and Data-Ethics CLE

Moderator: Amber Wilder, Associate Project Manager, Just-Tech

Speakers: Sandy Coyne, Deputy Director of Operations; Lori M. O'Brien, Esq., Deputy Director, Legal Assistance of Western New York, Inc.; Ellen Samuel, Director of Consulting, Just-Tech

Description: The presenters will discuss practical steps to bring your organization into compliance with the New York State Shield Act and reduce the risk of confidential data compromise. Presenters will discuss the ethics of cybersecurity, including a lawyer's duty of technological competence, protecting client confidentiality, and supervising third-party service providers. This session will include a discussion of security incidents involving legal aid organizations and how compliance with the Shield Act and other cybersecurity best practices would reduce the fall-out from such incidents.

Menu

Stop Hacks and Improve Electronic Data Security Act (“SHIELD Act”)

What is the significance of this law?

The SHIELD Act, signed into law on July 25, 2019 by Governor Andrew Cuomo, amends New York’s 2005 Information Security Breach and Notification Act. The Shield Act significantly strengthens New York’s data security laws by expanding the types of private information that companies must provide consumer notice in the event of a breach, and requiring that companies develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.

What types of security breaches are covered by this law?

Under the 2005 law, a security breach is defined as an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of private information. The SHIELD Act expands the definition of a security breach to any “access” to computerized data that compromises the confidentiality, security, or integrity of private data.

What does private information consist of?

Under the 2005 law, private information was any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver’s license number, account number, or credit or debit card number in combination with any required security code. The SHIELD Act expands the law to include biometric information, and username/email address and password credentials.

What are the safeguards that are included in the SHIELD Act?

The SHIELD Act requires any person or business that maintains private information to adopt administrative, technical and physical safeguards. Certain safeguards are listed but it is not meant to be an exhaustive list.

Reasonable administrative safeguards:

- designates one or more employees to coordinate the security program;
- identifies reasonably foreseeable internal and external risks;
- assesses the sufficiency of safeguards in place to control the identified risks;
- trains and manages employees in the security program practices and procedures;
- selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
- adjusts the security program in light of business changes or new circumstances.

Reasonable technical safeguards:

- assesses risks in network and software design;
- assesses risks in information processing, transmission and storage;
- detects, prevents and responds to attacks or system failures; and
- regularly tests and monitors the effectiveness of key controls, systems and procedures.

Reasonable physical safeguards:

- assesses risks of information storage and disposal;
- detects, prevents and responds to intrusions;
- protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

What are the obligations of businesses when a breach occurs?

The law requires that the person or business notify the affected consumers following discovery of the breach in the security of its computer data system affecting private information. The disclosure must be made in the most expedient time possible consistent with legitimate needs of law enforcement agencies. While the law requires notice to the Attorney General's office, New York Department of State and the New York State Police of the timing, content and distribution of the notices and approximate number of affected persons, submission of a breach form through the NYAG data breach reporting portal is sufficient as its automatically sent to all three entities: • Data Breach Reporting Portal

The person or business must also notify consumer reporting agencies if more than 5,000 New York residents are to be notified. The contact information for the three nationwide consumer reporting agencies is as follows:

EQUIFAX
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
www.equifax.com

EXPERIAN
Consumer Fraud Assistance
P.O. Box 9554
Allen, TX 75013
888-397-3742

www.experian.com

TRANSUNION
P.O. Box 2000
Chester, PA 19016-2000
Phone: 800-909-8872
www.transunion.com

If you are a consumer affected by a breach, you may **file a complaint through the Attorney General's online complaint form**. Do not submit a breach notification form.

Are there any exceptions to the notification requirements?

The law also provides for substitute notice to consumers if the business demonstrates to the Attorney General that the cost of providing regular notice would exceed $250,000 or that the affected class of persons exceeds 500,000 or the entity or business does not have sufficient contact information. Where substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity's web site, and notification to statewide media.

The law also does not require consumer notification if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

What are the penalties for violations of the SHIELD Act?

Under the SHIELD Act, the Attorney General may seek injunctive relief, restitution and penalties against any business entity for violating the law. For failure to provide timely notification, the court may impose a civil penalty of up to $20 per instance of failed notification not to exceed $250,000. For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to $5,000 per violation.

Bureau of Internet and Technology (BIT)

- Resource Center
  - File a Complaint
  - Consumer Education

- Privacy and Identity Theft
- Child Safety
- Buying Online
- Common Online Scams

- Report a Data Security Breach
- Initiatives
  - Anti-Child Pornography Initiatives
  - Electronic Security and Targeting of Online Predators Act (e-STOP)
  - Operation: Game Over
  - Report: Obstructed View: What's Blocking New Yorkers from Getting Tickets
  - Report: Airbnb in the city
  - Safety Model for Social Networking Sites

- Press Releases
- Contact

Search:

Please enter a search term...

STATE OF NEW YORK

5575--B

Cal. No. 1094

2019-2020 Regular Sessions

IN SENATE

May 7, 2019

Introduced by Sens. THOMAS, CARLUCCI, BIAGGI -- (at request of the Attorney General) -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged and said bill committed to the Committee on Consumer Protection -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, passed by Senate and delivered to the Assembly, recalled, vote reconsidered, restored to third reading, amended and ordered reprinted, retaining its place in the order of third reading

AN ACT to amend the general business law and the state technology law, in relation to notification of a security breach

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)".

§ 2. The article heading of article 39-F of the general business law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION**; DATA SECURITY PROTECTIONS**

§ 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899-aa of the general business law, subdivisions 1, 2, 3, 5, 6 and 7 as added by chapter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9 is renumbered subdivision 10 and a new subdivision 9 is added to read as follows:

1. As used in this section, the following terms shall have the following meanings:

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD05343-07-9

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean **either: (i)** personal information consisting of any information in combination with any one or more of the following data elements, when either the **data element or the combination of** personal information [~~or~~] **plus** the data element is not encrypted, or **is** encrypted with an encryption key that has also been **accessed or** acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

[~~or~~]

(3) account number, credit or debit card number, in combination with any required security code, access code, [~~or~~] password **or other information** that would permit access to an individual's financial account;

(4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized **access to or** acquisition **of,** or **access to or** acquisition without valid authorization**,** of computerized data that compromises the security, confidentiality, or integrity of [~~personal~~] **private** information maintained by a business. Good faith **access to, or** acquisition of [~~personal~~]**, private** information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which [~~conducts business in New York state, and which~~] owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, **accessed or** acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the system.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, **accessed or** acquired by a person without valid authorization.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons**, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account**;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him **or her** that there is a violation of this article he **or she** may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to [~~ten~~] **twenty** dollars per instance of failed notification, provided that the latter amount shall not exceed [~~one~~] **two** hundred fifty thousand dollars.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within [~~two~~] **three** years [~~immediately~~]

after either the date [~~of the act complained of or the date of discovery of such act~~] on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (b) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

§ 4. The general business law is amended by adding a new section 899-bb to read as follows:

§ 899-bb. Data security protections. 1. Definitions. (a) "Compliant regulated entity" shall mean any person or business that is subject to, and in compliance with, any of the following data security requirements:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

(b) "Private information" shall have the same meaning as defined in section eight hundred ninety-nine-aa of this article.

(c) "Small business" shall mean any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.

(b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either:

(i) is a compliant regulated entity as defined in subdivision one of this section; or

(ii) implements a data security program that includes the following:

(A) reasonable administrative safeguards such as the following, in which the person or business:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

(4) trains and manages employees in the security program practices and procedures;

(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and

(6) adjusts the security program in light of business changes or new circumstances; and

(B) reasonable technical safeguards such as the following, in which the person or business:

(1) assesses risks in network and software design;

(2) assesses risks in information processing, transmission and storage;

(3) detects, prevents and responds to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and

(C) reasonable physical safeguards such as the following, in which the person or business:

(1) assesses risks of information storage and disposal;

(2) detects, prevents and responds to intrusions;

(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

(4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

(c) A small business as defined in paragraph (c) of subdivision one of this section complies with subparagraph (ii) of paragraph (b) of subdivision two of this section if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers.

(d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fifty-d of this chapter.

(e) Nothing in this section shall create a private right of action.

§ 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8 of section 208 of the state technology law, paragraph (a) of subdivision 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005, subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as amended by chapter 491 of the laws of 2005, are amended and a new subdivision 9 is added to read as follows:

(a) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information [~~or~~] plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; [~~or~~]

(3) account number, credit or debit card number, in combination with any required security code, access code, [~~or~~] password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a

report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the

notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

§ 6. This act shall take effect on the ninetieth day after it shall have become a law; provided, however, that section four of this act shall take effect on the two hundred fortieth day after it shall have become a law.

RULE 1.1

COMPETENCE

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter, and whether it is feasible to associate with a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances. One such circumstance would be where the lawyer, by representations made to the client, has led the client reasonably to expect a special level of expertise in the matter undertaken by the lawyer.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all

legal problems. Perhaps the most fundamental legal skill consists of determining what kinds of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] [Reserved.]

[4] A lawyer may accept representation where the requisite level of competence can be achieved by adequate preparation before handling the legal matter. This applies as well to a lawyer who is appointed as counsel for an unrepresented person.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client may limit the scope of the representation if the agreement complies with Rule 1.2(c).

Retaining or Contracting with Lawyers Outside the Firm

[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 should reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. *See also* Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(g) (fee sharing with lawyers outside the firm), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the needs of the client; the education, experience and reputation of the outside lawyers; the nature of the services assigned to the outside 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.

[6A] Client consent to contract with a lawyer outside the lawyer's own firm may not be necessary for discrete and limited tasks supervised closely by a lawyer in the firm. However, a lawyer should ordinarily obtain client consent before contracting with an outside lawyer to perform substantive or strategic legal work on which the lawyer will exercise independent judgment without close supervision or review by the referring lawyer. For example, on one hand, a lawyer who hires an outside lawyer on a per diem basis to cover a single court call or a routing calendar call ordinarily would not need to obtain the client's prior informed consent. On the other hand, a lawyer who hires an outside lawyer to argue a summary judgment motion or negotiate key points in a transaction ordinarily should seek to obtain the client's prior informed consent.

[7] When lawyer from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other about the scope of their respective roles and the allocation of responsibility among them. *See* Rule 1.2(a). When allocating responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations (*e.g.*, under local court rules, the CPLR, or the Federal Rules of Civil Procedure) that are a matter of law beyond the scope of these Rules.

[7A] Whether a lawyer who contracts with a lawyer outside the firm needs to obtain informed consent from the client about the roles and responsibilities of the retaining and outside lawyers will depend on the circumstances. On one hand, if a lawyer retains an outside lawyer or law firm to work under the lawyer's close direction and supervision, and the retaining lawyer closely reviews the outside lawyer's work, the retaining lawyer usually will not need to consult with the client about the outside lawyer's role and level of responsibility. On the other hand, if the outside lawyer will have a more material role and will exercise more autonomy and responsibility, then the retaining lawyer usually should consult with the client. In any event, whenever a retaining lawyer discloses a client's confidential information to lawyers outside the firm, the retaining lawyer should comply with Rule 1.6(a).

[8] To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

RULE 1.4

COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of:

(i) any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required by these Rules;

(ii) any information required by court rule or other law to be communicated to a client; and

(iii) material developments in the matter including settlement or plea offers.

(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 a client's 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 these Rules 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.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client to participate effectively in the representation.

Communicating with Client

[2] In instances where these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with the client and secure the

client's consent prior to taking action, unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, paragraph (a)(1)(iii) requires that a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously made clear that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. *See* Rule 1.2(a).

[3] Paragraph (a)(2) requires that the lawyer reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases, the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Likewise, for routine matters such as scheduling decisions not materially affecting the interests of the client, the lawyer need not consult in advance, but should keep the client reasonably informed thereafter. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer or a member of the lawyer's staff acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications, or arrange for an appropriate person who works with the lawyer to do so.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should

review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interest and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(j).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. *See* Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to those who the lawyer reasonably believes to be appropriate persons within the organization. *See* Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

RULE 1.6

CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Comment

Scope of the Professional Duty of Confidentiality

[1] This Rule governs the disclosure of information protected by the professional duty of confidentiality. Such information is described in these Rules as "confidential information" as defined in this Rule. Other rules also deal with confidential information. See Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients; Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client; Rule 1.14(c) for information relating to representation of a client with diminished capacity; Rule 1.18(b) for the lawyer's duties with respect to information provided to the lawyer by a prospective client; Rule 3.3 for the lawyer's duty of candor to a tribunal; and Rule 8.3(c) for information gained by a lawyer or judge while participating in an approved lawyer assistance program.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source. See Rule 1.0(j) for the definition of informed consent. The lawyer's duty of confidentiality contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer,

even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Typically, clients come to lawyers to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is thereby upheld.

[3] The principle of client-lawyer confidentiality is given effect in three related bodies of law: the attorney-client privilege of evidence law, the work-product doctrine of civil procedure and the professional duty of confidentiality established in legal ethics codes. The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information or evidence concerning a client. The professional duty of client-lawyer confidentiality, in contrast, applies to a lawyer in all settings and at all times, prohibiting the lawyer from disclosing confidential information unless permitted or required by these Rules or to comply with other law or court order. The confidentiality duty applies not only to matters communicated in confidence by the client, which are protected by the attorney-client privilege, but also to all information gained during and relating to the representation, whatever its source. The confidentiality duty, for example, prohibits a lawyer from volunteering confidential information to a friend or to any other person except in compliance with the provisions of this Rule, including the Rule's reference to other law that may compel disclosure. *See* Comments [12]-[13]; *see also* Scope.

[4] Paragraph (a) prohibits a lawyer from knowingly revealing confidential information as defined by this Rule. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal confidential information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation with persons not connected to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client.

[4A] Paragraph (a) protects all factual information "gained during or relating to the representation of a client." Information relates to the representation if it has any possible relevance to the representation or is received because of the representation. The accumulation of legal knowledge or legal research that a lawyer acquires through practice ordinarily is not client information protected by this Rule. However, in some

circumstances, including where the client and the lawyer have so agreed, a client may have a proprietary interest in a particular product of the lawyer's research. Information that is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not "generally known" simply because it is in the public domain or available in a public file.

Use of Information Related to Representation

[4B] The duty of confidentiality also prohibits a lawyer from using confidential information to the advantage of the lawyer or a third person or to the disadvantage of a client or former client unless the client or former client has given informed consent. See Rule 1.0(j) for the definition of "informed consent." This part of paragraph (a) applies when information is used to benefit either the lawyer or a third person, such as another client, a former client or a business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not (absent the client's informed consent) use that information to buy a nearby parcel that is expected to appreciate in value due to the client's purchase, or to recommend that another client buy the nearby land, even if the lawyer does not reveal any confidential information. The duty also prohibits disadvantageous use of confidential information unless the client gives informed consent, except as permitted or required by these Rules. For example, a lawyer assisting a client in purchasing a parcel of land may not make a competing bid on the same land. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client, even to the disadvantage of the former client, after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(1).

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer may make disclosures of confidential information that are impliedly authorized by a client if the disclosures (i) advance the best interests of the client and (ii) are either reasonable under the circumstances or customary in the professional community. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. In addition, lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has

instructed that particular information be confined to specified lawyers. Lawyers are also impliedly authorized to reveal information about a client with diminished capacity when necessary to take protective action to safeguard the client's interests. See Rules 1.14(b) and (c).

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions that prevent substantial harm to important interests, deter wrongdoing by clients, prevent violations of the law, and maintain the impartiality and integrity of judicial proceedings. Paragraph (b) permits, but does not require, a lawyer to disclose information relating to the representation to accomplish these specified purposes.

[6A] The lawyer's exercise of discretion conferred by paragraphs (b)(1) through (b)(3) requires consideration of a wide range of factors and should therefore be given great weight. In exercising such discretion under these paragraphs, the lawyer should consider such factors as: (i) the seriousness of the potential injury to others if the prospective harm or crime occurs, (ii) the likelihood that it will occur and its imminence, (iii) the apparent absence of any other feasible way to prevent the potential injury, (iv) the extent to which the client may be using the lawyer's services in bringing about the harm or crime, (v) the circumstances under which the lawyer acquired the information of the client's intent or prospective course of action, and (vi) any other aggravating or extenuating circumstances. In any case, disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to prevent the threatened harm or crime. When a lawyer learns that a client intends to pursue or is pursuing a course of conduct that would permit disclosure under paragraphs (b)(1), (b)(2) or (b)(3), the lawyer's initial duty, where practicable, is to remonstrate with the client. In the rare situation in which the client is reluctant to accept the lawyer's advice, the lawyer's threat of disclosure is a measure of last resort that may persuade the client. When the lawyer reasonably believes that the client will carry out the threatened harm or crime, the lawyer may disclose confidential information when permitted by paragraphs (b)(1), (b)(2) or (b)(3). A lawyer's permissible disclosure under paragraph (b) does not waive the client's attorney-client privilege; neither the lawyer nor the client may be forced to testify about communications protected by the privilege, unless a tribunal or body with authority to compel testimony makes a determination that the crime-fraud exception to the privilege, or some other exception,

has been satisfied by a party to the proceeding. For a lawyer's duties when representing an organizational client engaged in wrongdoing, see Rule 1.13(b).

[6B] Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial risk that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims. Wrongful execution of a person is a life-threatening and imminent harm under paragraph (b)(1) once the person has been convicted and sentenced to death. On the other hand, an event that will cause property damage but is unlikely to cause substantial bodily harm is not a present and substantial risk under paragraph (b)(1); similarly, a remote possibility or small statistical likelihood that any particular unit of a mass-distributed product will cause death or substantial bodily harm to unspecified persons over a period of years does not satisfy the element of reasonably certain death or substantial bodily harm under the exception to the duty of confidentiality in paragraph (b)(1).

[6C] Paragraph (b)(2) recognizes that society has important interests in preventing a client's crime. Disclosure of the client's intention is permitted to the extent reasonably necessary to prevent the crime. In exercising discretion under this paragraph, the lawyer should consider such factors as those stated in Comment [6A].

[6D] Some crimes, such as criminal fraud, may be ongoing in the sense that the client's past material false representations are still deceiving new victims. The law treats such crimes as continuing crimes in which new violations are constantly occurring. The lawyer whose services were involved in the criminal acts that constitute a continuing crime may reveal the client's refusal to bring an end to a continuing crime, even though that disclosure may also reveal the client's past wrongful acts, because refusal to end a continuing crime is equivalent to an intention to commit a new crime. Disclosure is not permitted under paragraph (b)(2), however, when a person who may have committed a crime employs a new lawyer for investigation or defense. Such a lawyer does not have discretion under

paragraph (b)(2) to use or disclose the client's past acts that may have continuing criminal consequences. Disclosure is permitted, however, if the client uses the new lawyer's services to commit a further crime, such as obstruction of justice or perjury.

[6E] Paragraph (b)(3) permits a lawyer to withdraw a legal opinion or to disaffirm a prior representation made to third parties when the lawyer reasonably believes that third persons are still relying on the lawyer's work and the work was based on "materially inaccurate information or is being used to further a crime or fraud." *See* Rule 1.16(b)(1), requiring the lawyer to withdraw when the lawyer knows or reasonably should know that the representation will result in a violation of law. Paragraph (b)(3) permits the lawyer to give only the limited notice that is implicit in withdrawing an opinion or representation, which may have the collateral effect of inferentially revealing confidential information. The lawyer's withdrawal of the tainted opinion or representation allows the lawyer to prevent further harm to third persons and to protect the lawyer's own interest when the client has abused the professional relationship, but paragraph (b)(3) does not permit explicit disclosure of the client's past acts unless such disclosure is permitted under paragraph (b)(2).

[7] [Reserved.]

[8] [Reserved.]

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about compliance with these Rules and other law by the lawyer, another lawyer in the lawyer's firm, or the law firm. In many situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with these Rules, court orders and other law.

[10] Where a claim or charge alleges misconduct of the lawyer related to the representation of a current or former client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. Such a claim can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, such as a person claiming to have been defrauded by the lawyer and client acting together or by the lawyer acting alone. The lawyer may respond directly to the person who has made an accusation that permits disclosure, pro-

vided that the lawyer's response complies with Rule 4.2 and Rule 4.3, and other Rules or applicable law. A lawyer may make the disclosures authorized by paragraph (b)(5) through counsel. The right to respond also applies to accusations of wrongful conduct concerning the lawyer's law firm, employees or associates.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Paragraph (b) does not mandate any disclosures. However, other law may require that a lawyer disclose confidential information. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of confidential information appears to be required by other law, the lawyer must consult with the client to the extent required by Rule 1.4 before making the disclosure, unless such consultation would be prohibited by other law. If the lawyer concludes that other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

[13] A tribunal or governmental entity claiming authority pursuant to other law to compel disclosure may order a lawyer to reveal confidential information. Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason. In the event of an adverse ruling, the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge, unless such consultation would be prohibited by other law. If such review is not sought or is unsuccessful, paragraph (b)(6) permits the lawyer to comply with the order.

[14] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified in paragraphs (b)(1) through (b)(6). Before making a disclosure, the lawyer should, where practicable, first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose, particularly when accusations of wrongdoing in the representation of a client

have been made by a third party rather than by the client. If the disclosure will be made in connection with an adjudicative proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know the information, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[15] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may, however, be required by other Rules or by other law. *See* Comments [12]-[13]. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). *E.g.*, Rule 8.3(c)(1). Rule 3.3(c), on the other hand, requires disclosure in some circumstances whether or not disclosure is permitted or prohibited by this Rule.

Withdrawal

[15A] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw pursuant to Rule 1.16(b)(1). Withdrawal may also be required or permitted for other reasons under Rule 1.16. After withdrawal, the lawyer is required to refrain from disclosing or using information protected by Rule 1.6, except as this Rule permits such disclosure. Neither this Rule, nor Rule 1.9(c), nor Rule 1.16(e) prevents the lawyer from giving notice of the fact of withdrawal. For withdrawal or disaffirmance of an opinion or representation, see paragraph (b)(3) and Comment [6E]. Where the client is an organization, the lawyer may be in doubt whether the organization will actually carry out the contemplated conduct. Where necessary to guide conduct in connection with this Rule, the lawyer may, and sometimes must, make inquiry within the organization. *See* Rules 1.13(b) and (c).

Duty to Preserve Confidentiality

[16] Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information 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 otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to

current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients. Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.,* by making a device or 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. For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] 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. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked "Confidential" or "Confidential—Attorneys' Eyes Only"; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.

Lateral Moves, Law Firm Mergers, and Confidentiality

[18A] When lawyers or law firms (including in-house legal departments) contemplate a new association with other lawyers or law firms though lateral hiring or merger, disclosure of limited information may be necessary to resolve conflicts of interest pursuant to Rule 1.10 and to address financial, staffing, operational, and other practical issues. However, Rule 1.6(a) requires lawyers and law firms to protect their clients' confidential information, so lawyers and law firms may not disclose such information for their own advantage or for the advantage of third parties absent a client's informed consent or some other exception to Rule 1.6.

[18B] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter, including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each lawyer-client relationship; and (vi) information about aggregate current and historical payment of fees (such as realization rates, average receivables, and aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

[18C] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily *not* permitted, however, if information is protected by Rule 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney-client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness in paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; or information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

[18D] When lawyers are exploring a new association, whether by lateral move or by merger, all lawyers involved must individually consider fiduciary obligations to their existing firms that may bear on the timing and scope of disclosures to clients relating to conflicts and financial concerns, and should consider whether to ask clients for a waiver of confiden-

tiality if consistent with these fiduciary duties—*see* Rule 1.10(e) (requiring law firms to check for conflicts of interest). Questions of fiduciary duty are legal issues beyond the scope of the Rules.

[18E] For the unique confidentiality and notice provisions that apply to a lawyer or law firm seeking to sell all or part of its practice, see Rule 1.17 and Comment [7] to that Rule.

[18F] Before disclosing information regarding a possible lateral move or law firm merger, law firms and lawyers moving between firms—both those providing information and those receiving information—should use reasonable measures to minimize the risk of any improper, unauthorized or inadvertent disclosures, whether or not the information is protected by Rule 1.6(a), 1.9(c), or 1.18(b). These steps might include such measures as: (1) disclosing client information in stages; initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information outside the firm(s) during and after the lateral hiring negotiations or merger process.

RULE 5.1

RESPONSIBILITIES OF LAW FIRMS, PARTNERS, MANAGERS AND SUPERVISORY LAWYERS

(a) A law firm shall make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.

(b) (1) A lawyer with management responsibility in a law firm shall make reasonable efforts to ensure that other lawyers in the law firm conform to these Rules.

(2) A lawyer with direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the supervised lawyer conforms to these Rules.

(c) A law firm shall ensure that the work of partners and associates is adequately supervised, as appropriate. A lawyer with direct supervisory authority over another lawyer shall adequately supervise the work of the other lawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter, and the likelihood that ethical problems might arise in the course of working on the matter.

(d) A lawyer shall be responsible for a violation of these Rules by another lawyer if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the other lawyer practices or is a lawyer who has supervisory authority over the other lawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the con-

supervisory authority in particular circumstances is a question of fact. Partners and lawyers with comparable authority have at least indirect responsibility for all work being done by the firm, while a partner or manager in charge of a particular matter ordinarily also has supervisory responsibility for the work of other firm lawyers engaged in the matter. Partners and lawyers with comparable authority, as well as those who supervise other lawyers, are indirectly responsible for improper conduct of which they know or should have known in the exercise of reasonable managerial or supervisory authority. Appropriate remedial action by a partner or managing lawyer would depend on the immediacy of that lawyer's involvement and the seriousness of the misconduct. A supervisor is required to intervene to prevent misconduct or to prevent or mitigate avoidable consequences of misconduct if the supervisor knows that the misconduct occurred.

[6] Professional misconduct by a lawyer under supervision could reveal a violation of paragraph (a), (b) or (c) on the part of a law firm, partner or supervisory lawyer even though it does not entail a violation of paragraph (d) because there was no direction, ratification or knowledge of the violation or no violation occurred.

[7] Apart from this Rule and Rule 8.4(a), a lawyer does not have disciplinary liability for the conduct of another lawyer. Whether a lawyer may be liable civilly or criminally for another lawyer's conduct is a question of law beyond the scope of these Rules.

[8] The duties imposed by this Rule on managing and supervising lawyers do not alter the personal duty of each lawyer in a firm to abide by these Rules. *See* Rule 5.2(a).

RULE 5.2

RESPONSIBILITIES OF A SUBORDINATE LAWYER

(a) A lawyer is bound by these Rules notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate these Rules if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.

Comment

[1] Although a lawyer is not relieved of responsibility for a violation by the fact that the lawyer acted at the direction of a supervisor, that fact may be relevant in determining whether a lawyer had the knowledge required to render conduct a violation of these Rules. For example, if a subordinate filed a frivolous pleading at the direction of a supervisor, the subordinate would not be guilty of a professional violation unless the subordinate knew of the document's frivolous character.

[2] When lawyers in a supervisor-subordinate relationship encounter a matter involving professional judgment as to ethical duty, the supervisor may assume responsibility for making the judgment. Otherwise, a consistent course of action or position could not be taken. If the question can reasonably be answered only one way, the duty of both lawyers is clear, and they are equally responsible for fulfilling it. However, if the question is reasonably arguable, someone has to decide upon the course of action. That authority ordinarily reposes in the supervisor, and a subordinate may be guided accordingly. To evaluate the supervisor's conclusion that the question is arguable and the supervisor's resolution of it is reasonable in light of applicable Rules of Professional Conduct and other law, it is advisable that the subordinate lawyer undertake research, consult with a designated senior partner or special committee, if any (*see* Rule 5.1, Comment [3]), or use other appropriate means. For example, if a question arises whether the interests of two clients conflict under Rule 1.7, the supervisor's reasonable resolution of the question should protect the subordinate professionally if the resolution is subsequently challenged.

RULE 5.3

LAWYER'S RESPONSIBILITY FOR CONDUCT OF NONLAWYERS

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a lawyer who has supervisory authority over the nonlawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

Comment

[1] This Rule requires a law firm to ensure that work of nonlawyers is appropriately supervised. In addition, a lawyer with direct supervisory authority over the work of nonlawyers must adequately supervise

those nonlawyers. Comments [2] and [3] to Rule 5.1, which concern supervision of lawyers, provide guidance by analogy for the methods and extent of supervising nonlawyers.

[2] With regard to nonlawyers, who are not themselves subject to these Rules, the purpose of the supervision is to give reasonable assurance that the conduct of all nonlawyers employed by or retained by or associated with the law firm, including nonlawyers outside the firm working on firm matters, is compatible with the professional obligations of the lawyers and firm. Lawyers typically employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns and paraprofessionals. Such nonlawyer assistants, whether they are employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. Likewise, lawyers may employ nonlawyers outside the firm to assist in rendering those services. *See* Comment [6] to Rule 1.1 (retaining lawyers outside the firm). A law firm must ensure that such nonlawyer assistants are given appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose confidential information—*see* Rule 1.6 (c) (requiring lawyers to take reasonable care to avoid unauthorized disclosure of confidential information. Lawyers also should be responsible for the work done by their nonlawyer assistants. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline. A law firm should make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that nonlawyers in the firm and nonlawyers outside the firm who work on firm matters will act in a way compatible with the professional obligations of the lawyer. A lawyer with supervisory authority over a nonlawyer within or outside the firm has a parallel duty to provide appropriate supervision of the supervised nonlawyer.

[2A] Paragraph (b) specifies the circumstances in which a lawyer is responsible for conduct of a nonlawyer that would be a violation of these Rules if engaged in by a lawyer. For guidance by analogy, see Rule 5.1, Comments [5]-[8].

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include (i) retaining or contracting with an investigative or paraprofessional service, (ii) hiring a document management company to create and maintain a database for complex litigation, (iii) sending client documents to a third party for printing or scanning, and (iv) using an Internet-based service to

store client information. When using such services outside the firm, a lawyer or law firm must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of the reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the nonlawyer's work. *See also* Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4 (professional independence of the lawyer) and 5.5 (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer 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.

JUNE 2017

ABA Formal Opinion 477R: Securing communication of protected client information

Share:

Just this past week, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R (Revised May 22, 2017) on the subject of a lawyer's ethical obligations to protect confidential client information when transmitting information relating to the representation over the internet. The opinion takes a fresh look at advances in technology and ever-increasing cybersecurity threats, and provides guidance as to when enhanced security measures are appropriate.

This opinion is an update to ABA Formal Opinion 99-413 *Protecting the Confidentiality of Unencrypted E-Mail* (1999).

In 99-413, the committee concluded that since email provided a reasonable expectation of privacy, lawyers could use it to communicate with their clients, since it would be just as illegal to wiretap a telephone as it would be to intercept an email transmission. At the same time, the committee recognized that some information is so sensitive that a lawyer might consider using particularly strong protective measures depending on the sensitivity of the information:

> ... 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. – Formal Opinion 99-413 at page 2.

Since the time of Opinion 99-413, times have changed especially in the realm of technology and its many new and evolving manifestations that have become widespread in the profession. Laptop computers, smartphones, social media, cloud storage and Wi-Fi connections have become prevalent and much more commonplace than they were when 99-413 was written nearly 18 years ago.

The ABA Model Rules of Professional Conduct have also undergone several changes, particularly those that focus on a lawyer's obligation to protect client confidences when transmitting information over the internet.

Chief among these were the amendments to Rule 1.1 *Competence* and 1.6 *Confidentiality of Information* of the ABA Model Rules of Professional Conduct that were proposed by the ABA Ethics 20/20 Commission and subsequently adopted by the ABA House of Delegates at the 2012 ABA Annual Meeting. (The Ethics 20/20 Commission's Report and Recommendation concerning these amendments is available here.)

Paragraph 8 of the Comment to Rule 1.1 now states that "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology*..."

The commission also added a new subpart (c) to Rule 1.6 that states:

> **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.**

Paragraph 18 of the Comment to Rule 1.6 was also amended, making it clear that additional methods of security should be considered depending upon the sensitivity of the information that is to be transmitted.

In Opinion 477R, the committee took note of the increasing sophistication of cyber threats in today's technological environment and recognized that some new forms of electronic communication that have become commonplace may not in every instance provide a reasonable expectation of privacy:

> ...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 - Formal Opinion 477R at p. 5

In order to determine when additional security methods are required, the committee turned to the factors outlined in paragraph 18 of the Comment to Model Rule 1.6:

- 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).

The committee recommended the following steps lawyers should take to guard against disclosures, including:

1. Understand the nature of the threat. Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.

2. Understand how client confidential information is transmitted and where it is stored. Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.

3. Understand and use reasonable electronic security measures. Have an understanding of the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.

4. Determine how electronic communications about clients' matters should be protected. Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.

5. Label client confidential information. Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.

6. Train lawyers and nonlawyer assistants in technology and information security. Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.

7. Conduct due diligence on vendors providing communication technology. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.

TOPIC:

ETHICS

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

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[1]

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.[2] 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.[3] 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.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[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.

[2] *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).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

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,[6] 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.[7]

---

[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."[8] 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.)[9]

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]

---

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[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.[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

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

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[12] 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,[13] whether further action is warranted,[14] 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,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] 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.[17]

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

---

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).
[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").
[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.
[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

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.[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."[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

[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.").

[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> 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.[20]

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."[21] 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

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

[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).[22] 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.[23] 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."[24]

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).[25]

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.[26] 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.[27] 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.[28]

---

[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]

---

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[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.

---

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[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."[35] 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.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] 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.[38] 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.

Absent 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

---

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).
[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.").
[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).
[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

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.[40] 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 beach, 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.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] 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.[45]

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

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[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."

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 498 **March 10, 2021**

Virtual Practice

The ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm.[1] When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.

I. Introduction

As lawyers increasingly use technology to practice virtually, they must remain cognizant of their ethical responsibilities. While the ABA Model Rules of Professional Conduct permit virtual practice, the Rules provide some minimum requirements and some of the Comments suggest best practices for virtual practice, particularly in the areas of competence, confidentiality, and supervision. These requirements and best practices are discussed in this opinion, although this opinion does not address every ethical issue arising in the virtual practice context.[2]

II. Virtual Practice: Commonly Implicated Model Rules

This opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional brick-and-mortar law firm.[3] A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] Interstate virtual practice, for instance, also implicates Model Rule of Professional Conduct 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law, which is not addressed by this opinion. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 495 (2020), stating that "[l]awyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction."

[3] *See generally* MODEL RULES OF PROFESSIONAL CONDUCT R. 1.0(c), defining a "firm" or "law firm" to be "a lawyer or lawyers in a partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization on the legal department of a corporation or other organization." Further guidance on what constitutes a firm is provided in Comments [2], [3], and [4] to Rule 1.0.

have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need. Although the ethics rules apply to both traditional and virtual law practice,[4] virtual practice commonly implicates the key ethics rules discussed below.

A. Commonly Implicated Model Rules of Professional Conduct

1. Competence, Diligence, and Communication

Model Rules 1.1, 1.3, and 1.4 address lawyers' core ethical duties of competence, diligence, and communication with their clients. Comment [8] to Model Rule 1.1 explains, "To maintain the requisite knowledge and skill [to be competent], 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*). Comment [1] to Rule 1.3 makes clear that lawyers must also "pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor." Whether interacting face-to-face or through technology, lawyers must "reasonably consult with the client about the means by which the client's objectives are to be accomplished; . . . keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information. . . ."[5] Thus, lawyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually.[6]

2. Confidentiality

Under Rule 1.6 lawyers also have a duty of confidentiality to all clients and therefore "shall not reveal information relating to the representation of a client" (absent a specific exception, informed consent, or implied authorization). A necessary corollary of this duty is that lawyers must at least "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[7] The following non-

[4] For example, if a jurisdiction prohibits substantive communications with certain witnesses during court-related proceedings, a lawyer may not engage in such communications either face-to-face or virtually (e.g., during a trial or deposition conducted via videoconferencing). *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 3.4(c) (prohibiting lawyers from violating court rules and making no exception to the rule for virtual proceedings). Likewise, lying or stealing is no more appropriate online than it is face-to-face. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.15; MODEL RULES OF PROF'L CONDUCT R. 8.4(b)-(c).

[5] MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(2) – (4).

[6] Lawyers unexpectedly thrust into practicing virtually must have a business continuation plan to keep clients apprised of their matters and to keep moving those matters forward competently and diligently. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) (discussing ethical obligations related to disasters). Though virtual practice is common, if for any reason a lawyer cannot fulfill the lawyer's duties of competence, diligence, and other ethical duties to a client, the lawyer must withdraw from the matter. MODEL RULES OF PROF'L CONDUCT R. 1.16. During and following the termination or withdrawal process, the "lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred." MODEL RULES OF PROF'L CONDUCT R. 1.16(d).

[7] MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

exhaustive list of factors may guide the lawyer's determination of reasonable efforts to safeguard confidential information: "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)."[8] As ABA Formal Op. 477R notes, lawyers must employ a "fact-based analysis" to these "nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."

Similarly, lawyers must take reasonable precautions when transmitting communications that contain information related to a client's representation.[9] At all times, but especially when practicing virtually, lawyers must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information. This responsibility "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[10] However, depending on the circumstances, lawyers may need to take special precautions.[11] Factors to consider to assist the lawyer in determining the reasonableness of the "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."[12] As ABA Formal Op. 477R summarizes, "[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."

3. Supervision

Lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct.[13] Practicing virtually does not change or diminish this obligation. "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."[14] Moreover, a lawyer must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent

---

[8] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18].
[9] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].
[10] *Id.*
[11] The opinion cautions, however, that "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." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).
[12] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].
[13] MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3. *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 467 (2014) (discussing managerial and supervisory obligations in the context of prosecutorial offices). *See also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 n.6 (2018) (describing the organizational structures of firms as pertaining to supervision).
[14] MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [2].

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*."[15] The duty to supervise nonlawyers extends to those both within and outside of the law firm.[16]

B. Particular Virtual Practice Technologies and Considerations

Guided by the rules highlighted above, lawyers practicing virtually need to assess whether their technology, other assistance, and work environment are consistent with their ethical obligations. In light of current technological options, certain available protections and considerations apply to a wide array of devices and services. As ABA Formal Op. 477R noted, 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." Furthermore, "[o]ther available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems." To apply and expand on these protections and considerations, we address some common virtual practice issues below.

1. Hard/Software Systems

Lawyers should ensure that they have carefully reviewed the terms of service applicable to their hardware devices and software systems to assess whether confidentiality is protected.[17] To protect confidential information from unauthorized access, lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs). Finally, as technology inevitably evolves, lawyers should periodically assess whether their existing systems are adequate to protect confidential information.

---

[15] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (emphasis added).

[16] As noted in Comment [3] to Model Rule 5.3:

> When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including 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. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law).

[17] For example, terms and conditions of service may include provisions for data-soaking software systems that collect, track, and use information. Such systems might purport to own the information, reserve the right to sell or transfer the information to third parties, or otherwise use the information contrary to lawyers' duty of confidentiality.

2. Accessing Client Files and Data

Lawyers practicing virtually (even on short notice) must have reliable access to client contact information and client records. If the access to such "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."[18] Lawyers must ensure that data is regularly backed up and that secure access to the backup data is readily available in the event of a data loss. In anticipation of data being lost or hacked, lawyers should have a data breach policy and a plan to communicate losses or breaches to the impacted clients.[19]

3. Virtual meeting platforms and videoconferencing

Lawyers should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer's ethical obligations. Access to accounts and meetings should be only through strong passwords, and the lawyer should explore whether the platform offers higher tiers of security for businesses/enterprises (over the free or consumer platform variants). Likewise, any recordings or transcripts should be secured. If the platform will be recording conversations with the client, it is inadvisable to do so without client consent, but lawyers should consult the professional conduct rules, ethics opinions, and laws of the applicable jurisdiction.[20] Lastly, any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by other third parties who are not assisting with the representation,[21] to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality.

4. Virtual Document and Data Exchange Platforms

In addition to the protocols noted above (e.g., reviewing the terms of service and any updates to those terms), lawyers' virtual document and data exchange platforms should ensure that

---

[18] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018).

[19] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) ("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 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.'").

[20] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-422 (2001).

[21] Pennsylvania recently highlighted the following best practices for videoconferencing security:

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to "Host Only;"
- Ensure users are using the updated version of remote access/meeting applications.

Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2020-300 (2020) (citing an FBI press release warning of teleconference and online classroom hacking).

documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure. For example, if the lawyer is transmitting information over email, the lawyer should consider whether the information is and needs to be encrypted (both in transit and in storage).[22]

5. Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices

Unless the technology is assisting the lawyer's law practice, the lawyer should disable the listening capability of devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters. Otherwise, the lawyer is exposing the client's and other sensitive information to unnecessary and unauthorized third parties and increasing the risk of hacking.

6. Supervision

The virtually practicing managerial lawyer must adopt and tailor policies and practices to ensure that all members of the firm and any internal or external assistants operate in accordance with the lawyer's ethical obligations of supervision.[23] Comment [2] to Model Rule 5.1 notes that "[s]uch 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."

a. Subordinates/Assistants

The lawyer must ensure that law firm tasks are being completed in a timely, competent, and secure manner.[24] This duty requires regular interaction and communication with, for example,

---

[22] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) (noting that "it is not always reasonable to rely on the use of unencrypted email").

[23] As ABA Formal Op. 477R noted:

> 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.

[24] The New York County Lawyers Association Ethics Committee recently described some aspects to include in the firm's practices and policies:

- Monitoring appropriate use of firm networks for work purposes.
- Tightening off-site work procedures to ensure that the increase in worksites does not similarly increase the entry points for a data breach.
- Monitoring adherence to firm cybersecurity procedures (e.g., not processing or transmitting work across insecure networks, and appropriate storage of client data and work product).
- Ensuring that working at home has not significantly increased the likelihood of an inadvertent disclosure through misdirection of a transmission, possibly because the lawyer or nonlawyer was distracted by a child, spouse, parent or someone working on repair or maintenance of the home.

associates, legal assistants, and paralegals. Routine communication and other interaction are also advisable to discern the health and wellness of the lawyer's team members.[25]

One particularly important subject to supervise is the firm's bring-your-own-device (BYOD) policy. If lawyers or nonlawyer assistants will be using their own devices to access, transmit, or store client-related information, the policy must ensure that security is tight (e.g., strong passwords to the device and to any routers, access through VPN, updates installed, training on phishing attempts), that any lost or stolen device may be remotely wiped, that client-related information cannot be accessed by, for example, staff members' family or others, and that client-related information will be adequately and safely archived and available for later retrieval.[26]

Similarly, all client-related information, such as files or documents, must not be visible to others by, for example, implementing a "clean desk" (and "clean screen") policy to secure documents and data when not in use. As noted above in the discussion of videoconferencing, client-related information also should not be visible or audible to others when the lawyer or nonlawyer is on a videoconference or call. In sum, all law firm employees and lawyers who have access to client information must receive appropriate oversight and training on the ethical obligations to maintain the confidentiality of such information, including when working virtually.

b. Vendors and Other Assistance

Lawyers will understandably want and may need to rely on information technology professionals, outside support staff (e.g., administrative assistants, paralegals, investigators), and vendors. The lawyer must ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties. When appropriate, lawyers should consider use of a confidentiality agreement,[27] and should ensure that all client-related information is secure, indexed, and readily retrievable.

7. Possible Limitations of Virtual Practice

Virtual practice and technology have limits. For example, lawyers practicing virtually must make sure that trust accounting rules, which vary significantly across states, are followed.[28] The

---

- Ensuring that sufficiently frequent "live" remote sessions occur between supervising attorneys and supervised attorneys to achieve effective supervision as described in [New York Rule of Professional Conduct] 5.1(c).

N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 754-2020 (2020).

[25] *See* ABA MODEL REGULATORY OBJECTIVES FOR THE PROVISION OF LEGAL SERVICES para. I (2016).

[26] For example, a lawyer has an obligation to return the client's file when the client requests or when the representation ends. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.16(d). This important obligation cannot be fully discharged if important documents and data are located in staff members' personal computers or houses and are not indexed or readily retrievable by the lawyer.

[27] *See, e.g.*, Mo. Bar Informal Advisory Op. 20070008 & 20050068.

[28] *See* MODEL RULES OF PROF'L CONDUCT R. 1.15; *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) ("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

lawyer must still be able, to the extent the circumstances require, to write and deposit checks, make electronic transfers, and maintain full trust-accounting records while practicing virtually. Likewise, even in otherwise virtual practices, lawyers still need to make and maintain a plan to process the paper mail, to docket correspondence and communications, and to direct or redirect clients, prospective clients, or other important individuals who might attempt to contact the lawyer at the lawyer's current or previous brick-and-mortar office. If a lawyer will not be available at a physical office address, there should be signage (and/or online instructions) that the lawyer is available by appointment only and/or that the posted address is for mail deliveries only. Finally, although e-filing systems have lessened this concern, litigators must still be able to file and receive pleadings and other court documents.

III. Conclusion

The ABA Model Rules of Professional Conduct permit lawyers to conduct practice virtually, but those doing so must fully consider and comply with their applicable ethical responsibilities, including technological competence, diligence, communication, confidentiality, and supervision.

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.").

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

New York State Bar Association
Committee on Professional Ethics

Opinion 1240 (04/08/2022)

Topic: Duty to protect client information stored on a lawyer's smartphone.

Digest: If "contacts" on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent.

Rules: 1.6

FACTS:

1. When the inquiring lawyer downloads or accesses an app on his smartphone, the lawyer is sometimes asked whether the lawyer gives consent for that app to access the lawyer's "contacts" on the smartphone. The lawyer's contacts include clients in criminal representations.

QUESTION:

2. May a lawyer consent for an app to access contacts on the lawyer's smartphone that include the lawyer's current, former or prospective clients?

OPINION:

3. Rule 1.6(c) of the New York Rules of Professional Conduct (the "Rules") requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to" the confidential information of current, former and prospective clients. Rule 1.6(a), in turn, provides that confidential information "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

4. Rule 1.6(c) has been interpreted to require a lawyer to take reasonable care to protect clients' confidential information when carrying electronic devices containing such information across the border (see N.Y. City 2017-5 (2017)), when using an online storage provider to store clients' confidential information (see N.Y. State 842 (2010)), and when sending emails containing confidential information (see N.Y. State 709 (1998)).

5. In N.Y. State 820 (2008), we applied this general principle to a lawyer's use of an e-mail service provider that scans e-mails for keywords and sends or displays targeted computer-generated advertisements to the lawyer using the service based on the words in the e-mail communications. We concluded that using such a service is permissible if "[u]nder the particular e-mail provider's published privacy policies, no individuals other than e-mail senders and recipients read the e-mail messages, are otherwise privy to their content or receive targeted advertisements from the service provider." We reasoned: "Merely scanning the content of e-mails by computer to generate computer advertising . . . does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the emails' content." In contrast, we stated it would not be permissible to use the service "if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order)." Accordingly, we opined that a "lawyer must exercise due care in selecting an e-mail service provider to ensure that its policies and stated practices protect client confidentiality" in conformance with these governing principles.

6. In N.Y. State 1088 (2016), we addressed whether an attorney could disclose to a potential client the names of actual clients the attorney had represented in the same practice area. To answer that inquiry, we needed to determine, as a threshold matter, whether and under what circumstances the names of current or past clients could be "confidential information," as defined in Rule 1.6(a). We stated, first, that clients' names will be confidential information if the clients have requested keeping their names confidential. See N.Y. State 1088 ¶ 6 (2016). We then opined:

> If the client has not requested that the lawyer keep the client's name confidential, then the lawyer must determine whether the fact of representation is generally known and, if not, whether disclosing the identity of the client and the fact of representation is likely to be embarrassing or detrimental to the client. This will depend on the client and the specific facts and circumstances of the representation.

N.Y. State 1088 ¶ 7.

7. We discussed in Opinion 1088 what it meant to be "generally known" within the meaning of Rule 1.6(a) (¶ 8) and stated, "The client is more likely to find that disclosure of the fact of a current or prior representation by a lawyer is embarrassing or detrimental where the representation involves or involved criminal law, bankruptcy, debt collection or family law." Id. ¶ 9. Finally, we noted there might be other factors, other than the subject matter of the representation, that are relevant to determine whether the client would object to being identified as the lawyer's client. Id. ¶ 10.

8. Contacts stored on a smartphone typically include one or more email addresses, work or residence addresses, and phone numbers (collectively sometimes called "directory information"), but contacts often also include additional non-directory information (such as birth date or the lawyer's relationship to the contact). Social media apps may seek access to this information to solicit more users to the platform or to establish links between users and enhance the user experience. Apps which sell products or services may seek such access to promote additional sales. Apps that espouse political or social beliefs may seek such access to disseminate their views. These are but three examples of how an attorney's contacts might be exploited by an app, but there are more, and likely many more to come.

9. Insofar as clients' names constitute confidential information, a lawyer must make reasonable efforts to prevent the unauthorized access of others to those names, whether stored as a paper copy in a filing cabinet, on a smartphone, or in any other electronic or paper form. To that end, before an attorney grants access to the attorney's contacts, the attorney must determine whether any contact – even one – is confidential within the meaning of Rule 1.6(a). A contact could be confidential because it reflects the existence of a client-attorney relationship which the client requested not be disclosed or which, based upon particular facts and circumstances, would be likely to be embarrassing or detrimental to the client if disclosed. N.Y. State 1088 (2016).

10. Some relevant factors a lawyer should consider in determining whether any contacts are confidential are: (i) whether the contact information identifies the smartphone owner as an attorney, or more specifically identifies the attorney's area of practice (such as criminal law, bankruptcy law, debt collection law, or family law); (ii) whether people included in the contacts are identified as clients, as friends, as something else, or as nothing at all; and (iii) whether the contact information also includes email addresses, residence addresses, telephone numbers, names of family members or business associates, financial data, or other personal or non-public information that is not generally known.

11. If a lawyer determines that the contacts stored on his smartphone include the confidential information of any current or former client, the lawyer must not consent to give access to his contacts to an app, unless the attorney, after reasonable due diligence, including a review of the app's policies and stated practices to protect user information and user privacy, concludes that such confidential contact information will be handled in such a manner and for such limited purposes that it will not, absent the client's consent, be disclosed to additional third party persons, systems or entities. See N.Y. State 820 (2008).

CONCLUSION:

12. If "contacts" on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent.

(34-21)

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, New York 12207 ☐ PH 518.463.3200 ☐ www.nysba.org

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, *e.g.:*

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102(D) [now Rule 1.15(d)].
N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.
N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".
N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.
N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.
N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.
N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.
N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not

knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

> [17] 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. The duty 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 to 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 use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also noted, however, that "when the confidential information is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted internet e-mail." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving the use of "cloud" data storage, we were told that the storage system was password protected and that data stored in the system was encrypted. We concluded that the lawyer could

use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

> (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
>
> (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
>
> (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
>
> (4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, Locked Down: Information Security for Lawyers (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j).

7-14

NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. May a lawyer use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty? If so, what steps should the lawyer take to ensure that the information is sufficiently secure?

OPINION

2. Various companies offer online computer data storage systems that are maintained on an array of Internet servers located around the world. (The array of Internet servers that store the data is often called the "cloud.") A solo practitioner would like to use one of these online "cloud" computer data storage systems to store client confidential information. The lawyer's aim is to ensure that his clients' information will not be lost if something happens to the lawyer's own computers. The online data storage system is password-protected and the data stored in the online system is encrypted.

3. A discussion of confidential information implicates Rule 1.6 of the New York Rules of Professional Conduct (the "Rules"), the general rule governing confidentiality. Rule 1.6(a) provides as follows:

> A lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of a lawyer or a third person, unless:
>
> (1) the client gives informed consent, as defined in Rule 1.0(j);
>
> (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
>
> (3) the disclosure is permitted by paragraph (b).

4. The obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client's confidential information. *See* N.Y. County 733 (2004) (an attorney "must diligently preserve the client's confidences, whether reduced to digital format, paper, or otherwise"). As a New Jersey ethics committee observed, even when a lawyer wants a closed client file to be destroyed, "[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties." New Jersey Opinion (2006), *quoting* New Jersey Opinion 692 (2002).

5. In addition, Rule 1.6(c) provides that an attorney must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except to the extent disclosure is permitted by Rule 1.6(b). Accordingly, a lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney's supervision or who have been retained by the attorney to assist in providing services to the client. We note, however, that exercising "reasonable care" under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access.

6. To date, no New York ethics opinion has addressed the ethics of *storing* confidential information online. However, in N.Y. State 709 (1998) this Committee addressed the duty to preserve a client's confidential information when *transmitting* such information electronically. Opinion 709 concluded that lawyers may transmit confidential information by e-mail, but cautioned that "lawyers must always act reasonably in choosing to use e-mail for confidential communications." The Committee also warned that the exercise of reasonable care may differ from one case to the next. Accordingly, when a lawyer is on notice that the confidential information being transmitted is "of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer

must select a more secure means of communication than unencrypted Internet e-mail." *See also* Rule 1.6, cmt. 17 (a lawyer "must take reasonable precautions" to prevent information coming into the hands of unintended recipients when transmitting information relating to the representation, but is not required to use special security measures if the means of communicating provides a reasonable expectation of privacy).

7. Ethics advisory opinions in several other states have approved the use of electronic storage of client files provided that sufficient precautions are in place. *See, e.g.*, New Jersey Opinion 701 (2006) (lawyer may use electronic filing system whereby all documents are scanned into a digitized format and entrusted to someone outside the firm provided that the lawyer exercises "reasonable care," which includes entrusting documents to a third party with an enforceable obligation to preserve confidentiality and security, and employing available technology to guard against reasonably foreseeable attempts to infiltrate data); Arizona Opinion 05-04 (2005) (electronic storage of client files is permissible provided lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence"); *see also* Arizona Opinion 09-04 (2009) (lawyer may provide clients with an online file storage and retrieval system that clients may access, provided lawyer takes reasonable precautions to protect security and confidentiality and lawyer periodically reviews security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected).

8. Because the inquiring lawyer will use the online data storage system for the purpose of preserving client information - a purpose both related to the retention and necessary to providing legal services to the client - using the online system is consistent with conduct that this Committee has deemed ethically permissible. *See* N.Y. State 473 (1977) (absent client's objection, lawyer may provide confidential information to outside service agency for legitimate purposes relating to the representation provided that the lawyer exercises care in the selection of the agency and cautions the agency to keep the information confidential); *cf.* NY CPLR 4548 (privileged communication does not lose its privileged character solely because it is communicated by electronic means or because "persons necessary for the delivery or facilitation of such electronic communication may have access to" its contents).

9. We conclude that a lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or 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, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. *See* Rule 1.4 (mandating communication with clients); *see also* N.Y. State 820 (2008) (addressing Web-based email services).

11. Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *See, e.g.*, *City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619, 177 L.Ed.2d 216 (2010) (holding that City did not violate Fourth Amendment when it reviewed transcripts of messages sent and received by police officers on police department pagers); *Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. 2007) (e-mails between hospital employee and his personal attorneys were not privileged because employer's policy regarding computer use and e-mail monitoring stated that employees had no reasonable expectation of privacy in e-mails sent over the employer's e-mail server). *But see Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 990 A.2d 650 (2010) (despite employer's e-mail policy stating that company had right to review and disclose all information on "the company's media systems and services" and that e-mails were "not to be considered private or personal" to any employees, company violated employee's attorney-client privilege by reviewing e-mails sent to employee's personal attorney on employer's laptop through employee's personal, password-protected e-mail account).

12. This Committee's prior opinions have addressed the disclosure of confidential information in metadata and the perils of practicing law over the Internet. We have noted in those opinions that the duty to "exercise reasonable care" to prevent disclosure of confidential information "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks" in transmitting information electronically. N.Y. State 782 (2004), *citing* N.Y. State 709 (1998) (when conducting trademark practice over the Internet, lawyer had duty to "stay abreast of this evolving

technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost"); *see also* N.Y. State 820 (2008) (same in context of using e-mail service provider that scans e-mails to generate computer advertising). The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.

CONCLUSION

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

(75-09)

Cybersecurity, Privacy and Data Protection FAQs

The following Frequently Asked Questions (FAQs) relate to the changes in the New York State CLE Program Rules and the New York State CLE Board Regulations and Guidelines adding Cybersecurity, Privacy and Data Protection as a new CLE category of credit (effective January 1, 2023) and requiring that attorneys complete at least 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their biennial CLE requirement (effective July 1, 2023).

Experienced Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] Experienced attorneys (admitted to the New York Bar for more than two years) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their biennial CLE requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics.**

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that experienced attorneys must complete during each biennial reporting cycle?

A] No, experienced attorneys must still earn at least 24 CLE credit hours each biennial reporting cycle as follows:

Experienced Attorney Required CLE Categories **(for attorneys due to re-register on or after July 1, 2023)**	**Required CLE Credit Hours**
Ethics and Professionalism	4
Diversity, Inclusion and Elimination of Bias	1
Cybersecurity, Privacy and Data Protection (General or Ethics)	1*
Any CLE category of credit	18
Total Number of CLE credit hours	**24**

*You may choose to complete the Cybersecurity credit in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics**).

You may count a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 4-credit Ethics and Professionalism requirement.

- *Example*: if you earn 3 credits in Cybersecurity Ethics, then you still need to earn 1 credit in Ethics and Professionalism, 1 credit in Diversity, Inclusion and Elimination of Bias and 19 credits in any category of credit -- total of 24 credits

Q] When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] The new requirement becomes effective July 1, 2023.

- If you are **due to re-register on or after July 1, 2023 (birthday is on or after July 1st)**, you must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of your biennial CLE requirement.
- If you are **due to re-register in 2023 but your birthday is before July 1st**, you need **not** comply with the new requirement in 2023, but must comply in future biennial periods.
  - Example: If your birthday is on June 30th and you are due to re-register in 2023, then you do not need to comply with the new requirement in 2023, even if you file your registration form on or after July 1, 2023.
- If you are due to re-register in 2024, or later, you must comply with the new requirement.

Q] I'm due to re-register on or after July 1, 2023, but I won't be able to complete the Cybersecurity, Privacy and Data Protection requirement on time. What should I do?

A] You may apply for an extension of time to complete the CLE requirement.

Q] If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] May I satisfy any of my Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?

A] Yes, you may satisfy a maximum of 3 credits of your Ethics and Professionalism requirement with the same number of Cybersecurity, Privacy and Data Protection-Ethics credits.

Q] May I carry over Cybersecurity, Privacy and Data Protection CLE credits from one biennial reporting cycle to the next?

A] Yes. Once you have completed the 24-CLE credit requirement, a maximum of 6 additional credits earned may be applied toward the next reporting cycle. Experienced attorneys may carry over credits in any category, including Cybersecurity, Privacy and Data Protection, from one cycle to the next.

Newly Admitted Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] Newly admitted attorneys (admitted to the New York Bar for two years or less) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their newly admitted cycle requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics.**

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that newly admitted attorneys must complete during the newly admitted cycle?

A] No, newly admitted attorneys must still earn a total of 32 CLE credit hours (with 16 credit hours each year) in the newly admitted cycle as follows:

Newly Admitted Attorney Required CLE Categories (for attorneys admitted on or after July 1, 2023)	**Year 1 CLE Credit Hours**	**Year 2 CLE Credit Hours**
Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection-**General**	7 see below	7 see below
Skills	6	6
Ethics and Professionalism	3	3
Cybersecurity, Privacy and Data Protection-**Ethics**	see below	see below
Total Number of CLE credit hours	**16**	**16**

Cybersecurity, Privacy and Data Protection ("Cybersecurity") Category

- You must complete at least 1 credit in Cybersecurity as part of the 32-credit requirement.
- You may choose to complete the Cybersecurity credit:
  - in Year 1 or Year 2 (as part of the 16 credit-requirement for that year)
  - in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two)
- You may apply a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 6-credit Ethics and Professionalism requirement
  - *Example*: if you complete 1 credit in Cybersecurity **Ethics** in Year 1, you satisfy your Cybersecurity requirement, and then need to complete only 2 credits in Ethics and Professionalism for that year.
  - *Example*: if you complete 1 credit in Cybersecurity **General** in Year 1, you satisfy your Cybersecurity requirement and must complete an additional 6 credits in Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection-**General** for that year.

Q] When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] The new requirement becomes effective July 1, 2023 for attorneys **admitted to the NY Bar on or after** July 1, 2023.

- If you were admitted to the NY Bar **prior to July 1, 2023**, you need not comply with the Cybersecurity, Privacy and Data Protection requirement in your newly admitted cycle, but must comply in future reporting cycles.
- Attorneys admitted to the NY Bar **on or after July 1, 2023**, must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their newly admitted attorney CLE requirement.

Q] When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] Do I need to complete the Cybersecurity, Privacy and Data Protection CLE requirement in <u>each</u> year of my newly admitted cycle, i.e., 1 Cybersecurity CLE credit in Year 1 and 1 Cybersecurity CLE credit in Year 2?

A] No, you only need to complete 1 CLE credit in Cybersecurity, Privacy and Data Protection during your newly admitted cycle.

Q] Do I need to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement during the first or second year of my newly admitted cycle?

A] You can choose to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement in the first or second year of your newly admitted cycle as part of your 16-credit requirement for the year.

Q] May I carry over Cybersecurity, Privacy and Data Protection CLE credits?

A] Credit in Cybersecurity, Privacy and Data Protection-**Ethics** may **<u>not</u>** be carried over. Credit in Cybersecurity, Privacy and Data Protection-**General <u>may</u>** be carried over. For more information on carryover credit, please read the Newly Admitted FAQs.

Q] Do Cybersecurity, Privacy and Data Protection credits count toward my Ethics and Professionalism requirement?

A] You may count a maximum of 3 Cybersecurity, Privacy and Data Protection-**Ethics** credits toward your Ethics and Professionalism requirement in your newly admitted cycle. Cybersecurity, Privacy and Data Protection-**General** credits **do not** count toward your Ethics and Professionalism requirement.

Q] May I satisfy my entire Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?

A] No, you may satisfy a maximum of 3 credits of your total 6-credit Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-**Ethics** courses. By doing so, you would also satisfy your 1-credit Cybersecurity requirement.

Q] As a newly admitted attorney, in what formats can I take Cybersecurity, Privacy and Data Protection courses?

A] For Cybersecurity, Privacy and Data Protection-**General** courses, you may earn CLE credit in **any** approved format, including on-demand audio/video or webconference. For Cybersecurity, Privacy and Data Protection-**Ethics** courses, you may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Provider FAQs

Q] What may be addressed in Cybersecurity, Privacy and Data Protection programs?

A] Cybersecurity, Privacy and Data Protection CLE programs must relate to the practice of law, be specifically tailored to a legal audience, and aim to increase attorneys' professional ***legal*** competency. Please read Guidance for CLE Providers relating to Cybersecurity **Ethics** program areas and Cybersecurity **General** program areas.

Q] When may we begin to issue CLE credit in Cybersecurity, Privacy and Data Protection?

A] Providers may begin to issue credit in Cybersecurity, Privacy and Data Protection as of January 1, 2023, to attorneys who complete courses in this new category on or after January 1, 2023.

Q] What are the permissible formats for Cybersecurity, Privacy and Data Protection courses?

A] Experienced Attorneys: for Cybersecurity, Privacy and Data Protection (Ethics and General) courses, experienced attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.

Newly Admitted Attorneys:

- for Cybersecurity **General** courses, newly admitted attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.
- for Cybersecurity **Ethics** courses, newly admitted attorneys may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Q] We offered a live cybersecurity training in 2022 or earlier; can we issue CLE credit in the Cybersecurity, Privacy and Data Protection category to the attendees of this training?

A] No, you may not issue CLE credit in Cybersecurity, Privacy and Data Protection to the attendees of live courses that occurred prior to January 1, 2023.

Q] May we issue revised certificates awarding credit in the new Cybersecurity, Privacy and Data Protection category to attorneys who completed cybersecurity training in 2022 or earlier?

A] No. You may not issue revised certificates of attendance awarding credit in Cybersecurity, Privacy and Data Protection for courses completed prior to January 1, 2023.

Q] We issued CLE credit in Law Practice Management and Ethics and Professionalism for a course on cybersecurity in 2022 and we recorded the training. Can we issue CLE credit in the Cybersecurity, Privacy and Data Protection CLE category to participants who complete the prerecorded program on or after January 1, 2023?

A] Yes, assuming the content of the prerecorded program is timely and falls within the definition of Cybersecurity, Privacy and Data Protection, you can issue credit in Cybersecurity, Privacy and Data Protection to attorneys who complete the prerecorded program on or after January 1, 2023. Please note -- for newly admitted attorneys, the prerecorded format is permissible for credit in Cybersecurity, Privacy and Data Protection-**General** but not for credit in Cybersecurity, Privacy and Data Protection-**Ethics**.

Q] Can we issue CLE credit in Cybersecurity, Privacy and Data Protection training where there is no attorney faculty member participating?

A] No. As with all CLE programs, the faculty for a Cybersecurity, Privacy and Data Protection program should include an attorney in good standing who must actively participate in the program.

Q] Will there be a revised New York CLE Certificate of Attendance?

A] Yes, a revised New York CLE Certificate of Attendance that includes Cybersecurity, Privacy and Data Protection will be available on the CLE website and must be used beginning on January 1, 2023.