TECHNOLOGY COMPETENCE: THE NEW ETHICAL MANDATE FOR NORTH DAKOTA LAWYERS AND THE PRACTICE OF LAW

TRACY VIGNESS KOLB*

ABSTRACT

There is no obligation of lawyers more sacrosanct than protecting the confidential communications of the attorney-client relationship and maintaining the attorney-client privilege. Lawyers do not reveal client confidences and do not allow others, with whom confidences are entrusted, to do so either. It is an obligation easily understood and applied in the traditional settings of the practice of law. However, in today's world of electronic information, with client communications kept not just in file cabinets, but stored and transmitted electronically on laptops, smart phones, tablets, and in the cloud, client confidences are exposed to all the risks of an Internet connection.

It is the risks of technology and lawyers' increasing use of technology that prompted the American Bar Association to create the ABA Commission on Ethics 20/20 in 2009. The Ethics Commission studied the impact of technology and globalization on the legal profession in light of the very real and significant threats it posed to the privacy, security, and the confidentiality of attorney-client communications. The Ethics Commission's work resulted in proposed changes to the Model Rules of Professional Conduct (the "Technology Amendments") that were approved by the American Bar Association and, most of which, were adopted by the North Dakota Supreme Court effective March 1, 2016.

This Article examines the Technology Amendments and the new ethical obligations for North Dakota lawyers. The duty of competence now requires lawyers keep abreast of technology, while the duty of

* Tracy Vigness Kolb is a lawyer at Meagher & Geer in Bismarck, North Dakota. She has been practicing law in North Dakota since 1995 in the private and public sector handling litigation and legal and regulatory compliance matters, particularly in the health care law setting. Tracy has an in-depth working knowledge of HIPAA and HITECH and other data privacy and security laws, and has counseled clients and lawyers in their compliance efforts with these laws that includes developing data privacy and security programs. Among other privacy and security-related work and projects, Tracy was a member of the ABA's HITECH task force, a group of lawyers that worked over a five-year period studying and developing analyses, templates, forms and educational materials dealing with key HITECH privacy and security compliance issues.

confidentiality requires lawyers make reasonable efforts to prevent the impermissible use or disclosure of client confidences, not only by themselves but by others with whom they entrust client confidences. These are obligations to be competent in protecting and securing client confidences with reasonable security measures that address technology and the use of it. As encouraged by the American Bar Association, it is recommended that lawyers and law firms consider developing and implementing an information security program that addresses the privacy and security of client information and firm information systems consistent with these new ethical mandates.

I. INTRODUCTION

A most basic tenet of the professional responsibility of lawyers is protecting client confidences. It is "a fiduciary duty of the highest order."[1]

Protecting client confidences is an obligation lawyers have traditionally applied, and still do, in the "brick and mortar" setting of a physical office where paper files are stored in secured file cabinets behind locked office

1. *Resolution* 118 *and Report to the House of Delegates*, 2013 A.B.A. 5, Cybersecurity Legal Task Force, http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf [hereinafter *Resolution 118*].

doors. Client communications occur in person, on the phone, and through mailed letters. Of course these methods are still used today, but it is unlikely that there are lawyers who do not communicate with their clients electronically or store client communications on network servers[2] and mobile devices[3] that, with Internet services, are accessible anytime, anywhere. Today's technology has transformed the way lawyers communicate with clients and store client confidences, raising new confidentiality concerns and ethics issues, and requiring a new skill set for lawyers—technology competence.[4]

Technology competence is not a skill set lawyers are accustomed to or taught in law school. Twenty years ago, lawyers' use of technology consisted of a desktop computer, computerized legal research, and email. Today, essential technology skills require that lawyers: understand the cybersecurity risks and threats of an Internet connection and protect and secure client information accordingly; use the Internet consistent with ethical responsibilities for client development through websites, social media, and marketing; provide more efficient legal services using cloud-based systems to manage a legal practice; and conduct electronic discovery in litigation sometimes involving mass amounts of information requiring third-party investigative and document assembly and management services.[5]

Although lawyers are increasingly paying attention to information security and the application of safeguards in their use of technology, lawyers have room for improvement.[6] Because technology competence is now ethically mandated for North Dakota lawyers and the practice of law, there is no time like the present for lawyers to improve their technology skills.[7] The North Dakota Supreme Court adopted the Technology Amendments to the A.B.A. Model Rules of Professional Conduct that were proposed by the A.B.A. Commission on Ethics 20/20 and approved by the

2. Either a law firm server or third party server.

3. Including laptops, tablets, and smartphones.

4. *Introduction and Overvie*w, 2012 A.B.A. COMM'N ON ETHICS 3, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf [hereinafter *Ethics 20/20 Introduction and Overview*].

5. Andrew Perlman, *The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence*, *in* 22 PROF. LAW. 4, 1, 24 (2014), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/tpl_22_4.authcheckdam.pdf.

6. David Reis, *Security*, A.B.A. TechReport 2015, at 7, http://www.americanbar.org/content/dam/aba/publications/techreport/2015/security/Security.authcheckdam.pdf [hereinafter Reis, *Security*].

7. *Id.*

A.B.A. in August 2012.[8] The changes to the North Dakota Rules of Professional Conduct became effective March 1, 2016.[9]

II. THE CHARGE OF THE A.B.A. COMMISSION ON ETHICS 20/20

The ABA Commission on Ethics 20/20 (the "Ethics Commission") was created in 2009 by then-A.B.A. President Carolyn B. Lamm.[10] The Ethics Commission was charged with examining the impact of technology and globalization on the legal profession and determining whether changes to the A.B.A. Model Rules of Professional Conduct should be proposed.[11] The legal industry has been irrevocably changed by new technologies that pose threats to information security and privacy and to confidential communications between lawyers and their clients in ways that were unfathomable until recent years.[12]

A. TECHNOLOGY AND GLOBALIZATION

One of the areas of focus of the Ethics Commission was the confidentiality-related concerns arising from two types of technology used by lawyers to store and transmit electronic information. The first type of technology is "local" technology, which is controlled by lawyers and their employees, such as mobile devices, network servers, and office equipment like copiers.[13] The second type of technology is cloud computing and outsourcing services, which are controlled by third parties and accessed over the Internet.[14] These services include online data storage, Internet-based email, and Software as a Service ("SaaS").[15] Outsourcing concerns, however, were not limited to cloud-based services. These concerns also

---

8. N.D. Sup. Ct. Admin. R. § 6.1 (2014) (amended 2016), https://www.ndcourts.gov/Court/Notices/20160245/ar6.1.htm; N.D. Sup. Ct. Admin. R. § 46 (2014) (amended 2016), https://www.ndcourts.gov/Court/Notices/20160245/ar46.htm.

9. *Id*.

10. AM. BAR ASS'N, *A B.A. Commission on Ethics 20/20*, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited July 15, 2016).

11. *Memorandum*, AM. BAR. ASS'N, *Re: Summary of Actions by the A B.A. Commission on Ethics 20*/20, (Dec. 28, 2011), at 1. North Dakota Supreme Court Chief Justice Gerald VandeWalle was a member of the Commission.

12. The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, at 3 (Nov. 2015) [hereinafter Sedona Conference, *Guidelines for Lawyers*].

13. *Memorandum*, AM. BAR ASS'N, *Re: For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology*, 3-4 (Sept. 20, 2010).

14. *Id*. at 2.

15. *Id*. at 1. Software as a Service is software accessed over the Internet and is sold on a subscription basis, unlike traditional software which is purchased per license and installed on a computer or network.

included the increased use of outside lawyers and non-lawyers performing legal tasks, such as forensic investigators conducting electronic discovery and other vendors and service providers conducting services for law firms.[16]

The work of the Ethics Commission relating to technology and outsourcing resulted in proposed amendments to Model Rules of Professional Conduct 1.0, 1.1, 1.4, 1.6, 4.4, 5.3, and 5.5.

The Ethics Commission also addressed ethical issues arising from lawyers' use of Internet-based client development tools, such as social networking, law firm websites, and blogs.[17] In addition, the Ethics Commission discussed the globalization of the legal marketplace facilitated by technology and the Internet, and the ensuing ethical issues involving cross-jurisdictional practice and lawyer mobility.[18]

The work of the Ethics Commission related to client development and globalization resulted in proposed amendments to Model Rules of Professional Conduct 1.6, 1.17, 1.18, 5.5, 7.1, 7.2, and 7.3.

The A.B.A. approved the Ethics Commissions' proposed amendments on August 6, 2012.[19]

III. THE NEW RULES: TECHNOLOGY-CONFIDENTIALITY AND OUTSOURCING

The North Dakota Supreme Court adopted most of the rule changes proposed by the Ethics Commission and approved by the A.B.A.[20] Below, this Article discusses the Technology Amendments to Rules 1.0, 1.1, 1.6, 4.5, and 5.3. Lawyers should also familiarize themselves with the changes made to Rules 1.17, 1.18, 5.5, 7.1, 7.2, and 7.3 because there is new guidance regarding, among other things, when an electronic communication gives rise to a prospective lawyer-client relationship and when a lawyer's online communication constitutes direct solicitation of a client.[21] A discussion of the changes to these Rules pertaining to client development is beyond the scope of this Article.

---

16. *Id*. at 3-4.

17. *Memorandum*, AM. BAR. ASS'N, *Re: For Comment: Issues Paper Concerning Lawyers' Use of Internet Based Development Tools*, (Sept. 20, 2010), at 1.

18. *Ethics 20/20 Introduction and Overview*, *supra* note 4, at 5-7.

19. For a discussion of the Model Rules amendments regarding technology, outsourcing, client development and lawyer mobility, see the A.B.A.'s website, A.B.A. COMMISSION ON ETHICS 20/20, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited July 12, 2016).

20. North Dakota Supreme Court Order of Adoption, Sup. Ct. No. 20150186 (Dec. 9, 2015).

21. N.D. RULES OF PROF'L. CONDUCT r. 1.17, 1.18, 5.5, 7.2, & 7.3 (2016).

A. PROTECT AND MAINTAIN CLIENT CONFIDENCES

The rules that directly impact the ethical obligations of lawyers to protect and secure client information are Rules 1.0, 1.1, 1.6, 4.5, and 5.3. Under the changes made to these Rules, lawyers are now required to maintain competence in protecting and securing client confidences with reasonable security measures that address technology and the use of it.[22]

1. *The Duty of Competence*

Rule 1.0, concerning Terminology, has been amended to explain that the term "writing" is not limited only to email, but includes all other forms of electronic communications.[23] Additional clarification was added to explain that screening of disqualified lawyers applies not only to documents, but to information in electronic form.[24]

Rule 1.1 requires a lawyer provide competent representation to a client.[25] Competent representation includes keeping abreast of changes in technology.[26] Comment [5] to Rule 1.1 provides: "To maintain the requisite knowledge and skill, a lawyer must 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."[27]

This obligation of technology competence requires that lawyers become and remain competent about the technology they use as well as the benefits and risks associated with its use.[28] It is not an obligation mandating that a lawyer personally have all the needed technology competencies, but it does require lawyers to better understand and be able to use technology, and, if necessary, consult with appropriately-qualified individuals, like Information Technology ("IT") experts for advice in using particular aspects of technology.[29]

---

22. N.D. RULES OF PROF'L. CONDUCT r.1.0, 1.1, 1.6, 4.5, & 5.3 (2016).
23. N.D. RULES OF PROF'L. CONDUCT r.1.0 (2015).
24. N.D. RULES OF PROF'L. CONDUCT r.1.0 cmt 7 (2015).
25. N.D. RULES OF PROF'L. CONDUCT r.1.1 (2015).
26. *Id.*
27. N.D. RULES OF PROF'L. CONDUCT r.1.1 (2015) (emphasis added).
28. *Ethics 20/20 Introduction and Overview*, *supra* note 4, at 8. Staying informed about technology has been implicitly understood as encompassed in the lawyer's obligation to maintain competence by keeping abreast of changes in the law and its practice. *Id.* Comment [5] clarifies expressly what has previously been understood about a lawyer's obligation to provide competent representation.
29. JILL D. RHODES & VINCENT I. POLLEY, ABA CYBERSECURITY LEGAL TASKFORCE, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS, 66 (2013) [hereinafter *ABA Cybersecurity Handbook*]. North Dakota Supreme Court Justice Daniel Crothers is a contributing author to the ABA Cybersecurity Handbook.

2. *The Duty of Confidentiality*

Under Rule 1.6(a), lawyers have a duty not to reveal client confidences, no matter the source, form, or media, whether electronic, paper, or oral.[30] Lawyers now have an additional ethical obligation "to *prevent* such a revelation."[31] New paragraph (d) to Rule 1.6 provides: "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."[32] This rule is best understood as an obligation to *secure* client information.

To further understand the obligation, Comment [18] to Rule 1.6 has been amended to include, among other things, factors for lawyers to consider in determining whether their information security efforts to protect and secure client information are reasonable.[33] Those factors are: (1) the sensitivity of the information; (2) the likelihood of disclosure if additional safeguards are not employed; (3) the cost of employing additional safeguards; (4) the difficulty of implementing the safeguards; and (5) 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).[34]

Reasonable efforts to prevent impermissible uses or disclosures of client information will require that lawyers implement security measures,

---

30. N.D. RULES OF PROF'L. CONDUCT r.1.6(a) (2015). In addition, lawyers may not reveal metadata contained in electronic documents. Seventeen states have addressed the ethical issue of metadata in electronic documents and have concluded that "lawyers have an obligation to understand the technology that they utilize and a lawyer sending files in an electronic format must exercise reasonable care in transmitting files in electronic format so as not to disclose client confidences." *Ethics Opinion No. 259*, 2012 MISS.B. ETHICS COMM. 4, http://msbar.org/media/583222/Formal%20Opinion%20259.pdf (qualifying application of opinion to "electronic documents which are voluntarily provided by one attorney to another attorney" because "metadata contained in electronic documents provided in response to discovery requests or pursuant to a subpoena are . . . subject to applicable court rules"); *see* State v. Ratliff, 2014 ND 156, ¶¶ 37-43, 849 N.W.2d 183, 193-96 (Crothers, J., concurring) (discussing the increased vigilance required of lawyers and judges when introducing and admitting electronic information that may contain metadata). The A.B.A. maintains states' metadata ethics opinions on its website, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

31. N.D. RULES OF PROF'L. CONDUCT r.1.6(d) (2015) (emphasis added); *Resolution 105A and Report*, 2012 A.B.A. COMM'N ON ETHICS 20/20 4, https://isb.idaho.gov/pdf/sections/pro/pro_abaresolutions105a-f.pdf12 [hereinafter *Resolution 105A and Report*].

32. N.D. RULES OF PROF'L. CONDUCT r.1.6(d) (2015).

33. N.D. RULES OF PROF'L. CONDUCT r.1.6(d) cmt. 18 (2015).

34. *Id.*

such as reasonably available administrative, technical, and physical safeguards.[35]

Administrative, physical, and technical safeguards are information security measures known to lawyers who perform legal services for health care clients that are covered entities subject to the Health Insurance Portability and Accountability Act ("HIPAA").[36] As business associates of covered entities, these lawyers have been required to comply with HIPAA's Privacy and Security Rule since February 2010, when the Health Information Technology for Economic and Clinical Health Act ("HITECH") extended HIPAA's application to business associates, including lawyers and law firms.[37] These lawyers and law firms have already established an information security program, including implementing the fifty-three standards and specifications that constitute HIPAA's administrative, physical, and technical safeguards.[38] Lawyers with clients in the financial services industry also have faced complex compliance obligations under the "Safeguards Rule" of the Gramm-Leach-Bliley Act ("GLBA").[39] Like HIPAA's Security Rule, the Safeguards Rule imposes obligations on lawyers and law firms that handle information covered by GLBA to implement administrative, technical, and physical

---

35. *Resolution 105A and Report*, *supra* note 31, at 4. Comment [16] to Rule 1.6 addresses a lawyer's obligation when storing confidential information whereas Comment [17] addresses the obligation when transmitting confidential information, such as by email. *Compare* N.D. RULES OF PROF'L. CONDUCT r.1.6 cmt. 16, *with* N.D. RULES OF PROF'L. CONDUCT r. 1.6 cmt. 17.

36. 45 C.F.R. Parts 160, 162, 164 (2016).

37. Under HIPAA, administrative safeguards are "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information." 45 C.F.R. § 164.304 (2016). Physical safeguards are "physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion" and includes any physical locations outside of an actual office, such as home computers and mobile devices. *Id*. "Technical safeguards" means "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." *Id*. I wrote about this compliance obligation of lawyers in The Gavel in November 2009. *See* Tracy Vigness Kolb, *"What is HITECH?,"* THE GAVEL, ST. B. ASS'N OF N.D., Nov. 2009; *see also* Tracy Vigness Kolb, *A Resource Guide: The HIPAA Privacy and Security Rule, Enforcement Rule, and HITECH Breach Notification Rule and North Dakota State Breach Notification Law*, Version 1 (2016); *Cross-walk Between Current Business Associate Agreement and New HITECH Act Requirements*, Security Compliance for Business Associates Subcommittee, ABA Health Law Section HITECH Task Force, Nov. 2009, Reissued May 2013 (Contributing Member of Subcommittee); Tracy Vigness Kolb, *"Will You Be Ready For HITECH Health Care?,"* CHECK UP, N.D. Medical ASS'N, June 2009.

38. 45 C.F.R. Part 164, Subparts A, C (2016).

39. *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), http://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

safeguards.[40] Other lawyers and law firms not subject to HIPAA, GLBA, or other federal or state laws should evaluate their information security practices and implement appropriate measures based on the new factors provided in Comment [18] to Rule 1.6.[41]

Importantly, the Ethics Commission recognized that this ethical obligation is not synonymous to the legal, regulatory, or contractual obligations of lawyers and law firms, as with those obligations imposed on business associate lawyers and law firms under HIPAA.[42] Other than enumerating the factors under Comment [18] to Rule 1.6, the Ethics Commission declined to propose more specific guidance about the "reasonable efforts" that lawyers should employ because technology advances too rapidly and lawyers will need to keep up with the pace of change and respond with appropriate measures as technologies evolve and new risks emerge.[43] This, therefore, explains the new provision under Comment [18] which reminds lawyers that, in addition to their ethical obligations, there are laws and regulations that impose confidentiality-related obligations.[44] It is doubtful that North Dakota lawyers and law firms are not subject to one or more laws, especially at the state level, which impose some sort of legal data protection or breach notification requirements beyond the ethical obligation of Rule 1.6(d).

In addition to federal breach notification laws, such as HIPAA, North Dakota and forty-six other states have a state breach notification law.[45] This law applies to any person who owns, licenses, or maintains computerized personal information about a North Dakota resident regardless of where that person conducts business.[46] Personal information means an individual's first name or first initial and last name in combination with any other enumerated data element, such as a social security number, driver's license number, date of birth, or medical information.[47] Notification is triggered if there is a security system breach,

---

40. Sedona Conference, *Guidelines for Lawyers*, *supra* note 12, at B-4.

41. N.D. RULES OF PROF'L. CONDUCT r.1.6(d) cmt. 18 (2015).

42. 45 C.F.R. § 160.103 (2016) (defining "business associate" to include a person who provides legal services to a covered entity).

43. *Resolution 105A and Report*, *supra* note 31, at 5.

44. N.D. RULES OF PROF'L. CONDUCT r.1.6(d) cmt. 18 (2015):

> Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information is beyond the scope of these Rules.

45. N.D. CENT. CODE § 51-30 (2015).

46. N.D. CENT. CODE §§ 51-30-02 to 51-30-03 (2015).

47. *Id.* § 51-30-01.

which means the "unauthorized acquisition of computerized data that includes personal information."[48] North Dakota's breach notification law applies to both lawyers and law firms.[49] Breach notification laws of other states may also apply if a breach involves personally identifiable information about residents of another state.[50]

If a data breach occurred involving client information, a lawyer would likely be obligated to inform the client under Rule 1.4, which addresses a lawyer's duty to communicate with a client.[51]

The new ethical obligation under Rule 1.6(d) does not include an expectation that lawyers "achieve the unattainable" and guarantee electronic security of client confidences.[52] Instead, a lawyer's efforts at protecting and securing those confidences will be measured by the reasonableness of the efforts to prevent an impermissible use or disclosure.[53] If, despite reasonable efforts, there is a breach of client information, there will not be a violation of Rule 1.6(d).[54]

Together, the Technology Amendments to Rules 1.1 and 1.6 require lawyers using technology to take competent and reasonable measures to safeguard client information.[55] This duty extends to the use of all technology, including desktop and laptop computers, mobile devices, network servers, cloud computing, and outsourcing.[56]

---

48. *Id*. § 51-30-01(1). Notification, however, is not required if the data was secured by encryption or any other method of technology that renders the electronic files, media, or databases unreadable or unusable. *Id*. Breach does not include, and, therefore, notification is not required for, the good faith acquisition of personal information by an employee or agent of the person, if the personal information is not used or subject to further unauthorized disclosure. *Id*.

49. *Id*. §§ 51-30-02 to 51-30-03 (applying to any person that owns, licenses, or maintains computerized data).

50. The American Health Lawyers Association has published a fifty-state survey of state data breach notification laws. LEXISNEXIS, *AHLA Data Breach Notification Laws: A Fifty State Survey, Second Edition (AHLA Members)*, http://www.lexisnexis.com/ahla/ProductDetail.aspx?id=32 (last visited July 12, 2016).

51. N.D. RULES OF PROF'L. CONDUCT r.1.4 (2015). Communicating with a client about security measures has gained growing importance in light of the Technology Amendments, in particular a new sentence under Comment [18] of Rule 1.6 that provides: "A client may require the lawyer to implement special security measures not required by this Rule or may consent to forgo security measures that would otherwise be required by this Rule." This provision necessarily contemplates that there is a discussion between a lawyer and client about security measures the lawyer uses for protecting and securing client information, including electronic communications with the client. It has been suggested the lawyer should initiate that "cybersecurity" discussion with the client at the beginning of the representation. *ABA Cybersecurity Handbook*, *supra* note 29, at ch. 3, Sec. III.B & C.

52. *Ethics 20/20 Introduction and Overview*, *supra* note 4, at 8.

53. N.D. RULES OF PROF'L. CONDUCT r.1.6(d), cmt. 18 (2015).

54. *Id*.

55. N.D. RULES OF PROF'L. CONDUCT r. 1.1, 1.6(d) (2015).

56. *Id*.

One particular ethics issue associated with inadvertent disclosure is addressed in Rule 4.5, which requires that the lawyer who receives a document relating to the representation of a lawyer's client, and knows or should know the document was inadvertently sent, must notify the sender.[57] This rule was amended to replace the word "document" with the phrase "document or electronically stored information."[58] For clarification, the phrase "inadvertently sent" was defined, under Comment [1] of Rule 4.5, to mean a document that was accidently transmitted.[59] Examples of an accidental transmission include "when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted."[60]

B. ENSURING OTHERS PROTECT AND MAINTAIN CLIENT CONFIDENCES

Under Rule 5.1, partners and managing lawyers in a law firm have a duty of supervision which includes that the firm make reasonable efforts to ensure lawyers in the firm comply with their ethical obligations.[61] In light of lawyers' increasing use of vendors, service providers, and the outsourcing of legal work to lawyers and non-lawyers, comments to Rules 1.1 and 5.3 have been amended to underscore that this supervisory responsibility extends to non-lawyers within and outside a firm, and lawyers outside a firm, to ensure they use technology in a manner that reasonably safeguards client information entrusted to them.[62]

Outsourcing is the practice of engaging others outside a law firm to provide a function, activity, or service often performed within the firm.[63] Examples of outsourced legal work include investigative services, Internet data storage at an offsite location, and Internet based "practice management tools" such as cloud computing services.[64] Outsourcing by lawyers also

---

57. N.D. RULES OF PROF'L. CONDUCT r. 4.5 (2016).

58. *Id*.

59. N.D. RULES OF PROF'L. CONDUCT r. 4.5 cmt. 1 (2016).

60. *Id*.

61. N.D. RULES OF PROF'L. CONDUCT r. 5.1(a) (2015). Efforts that satisfy this rule include developing information security practices and policies to maintain client confidences, establishing appropriate uses of mobile devices and the Internet, and employee training. *See* N.D. RULES OF PROF'L. CONDUCT r. 5.1(a) cmts. 1, 2, & 3 (2015); *Resolution 109 and Report to the House of Delegates*, 2014 A.B.A. 1, Cybersecurity Legal Task Force, https://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf [hereinafter *Resolution 109*].

62. *Ethics 20/20 Introduction and Overview*, *supra* note 4, at 12.

63. *Resolution 105C and Report*, 2012 A.B.A. COMM'N ON ETHICS 20/20, at 2, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

64. *Id*.

includes the use of vendors and service providers outside a law firm, such as third-party IT providers and shredding and copier maintenance companies.[65]

Two new comments were added to Rule 1.1 to impress upon lawyers their ethical obligation to ensure confidentiality when retaining lawyers outside the firm to assist on a client's matter. A lawyer's decision to retain or contract with a lawyer outside the firm will be measured by its reasonableness, considering circumstances such as "the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, *particularly relating to confidential information*."[66]

Comment [2] to Rule 5.3 was amended to require that managing lawyers of a law firm make reasonable efforts to ensure that non-lawyers within and outside a firm, perform their work on behalf of the firm, which when using technology, includes appropriately handling and securing client information.[67]

Two new comments were also added to Rule 5.3 to specifically address the use of non-lawyers outside a firm and their handling and safeguarding of client information.[68] When lawyers use non-lawyers outside a firm to assist in providing legal services to a client, the lawyer's decision to do so will be measured by its reasonableness considering the same circumstances as those for lawyers outside a firm.[69] However, for non-lawyers, the lawyer should "communicate directions appropriate under the circumstances" to ensure the non-lawyer appropriately handles and safeguards confidential information.[70]

To communicate appropriate directions to non-lawyers outside a firm, lawyers should, and in some instances must (for example, business associate subcontractors under HIPAA) consider written agreements that govern the provisions of the non-lawyer's services, specifically addressing their use of technology.[71] Possible terms and conditions to address when contracting cloud-based services, for example, include the ownership and physical location of stored data; the provider's backup policies; the accessibility of stored data by the provider's employees or sub-contractors; the provider's compliance with particular state and federal laws governing

65. *Id*.
66. N.D. RULES OF PROF'L. CONDUCT r.1.1 cmts. 7, 8 (2015) (emphasis added).
67. N.D. RULES OF PROF'L. CONDUCT r. 5.3 cmt. 2 (2015).
68. N.D. RULES OF PROF'L. CONDUCT r. 5.3 cmts. 7, 8 (2015).
69. *Id*. cmt. 7.
70. *Id*.
71. *E.g*., 45 C.F.R. § 164.502(e)(2) (2016).

data privacy (including notifications regarding security breaches); the format of the stored data (and whether it is compatible with software available through other providers); the type of data encryption; and policies regarding the retrieval of data upon the termination of services.[72] These types of terms and conditions are important to ensure the lawyer understands how the provider will safeguard the entrusted confidential information.

Vendor management, including cloud-based providers, has become a heightened concern because of the frequency of data breaches that involve vendors and the increased use of cloud services and outsourcing by lawyers.[73] Currently, there are twenty state bar associations, including the State Bar Association of North Dakota, that have addressed the use of cloud computing or cloud storage.[74] There are some differences in the state bar association opinions, but generally each permits a lawyer to use the cloud.[75] Some opinions are very detailed in discussing the measures lawyers should take to select and use a cloud vendor.[76] New York, for example, requires lawyers to exercise reasonable care to ensure the cloud provider's system is secure and client confidentiality will be maintained.[77] According to the New York opinion, reasonable care may mean: (1) requiring an enforceable obligation with the provider to preserve confidentiality and security, including notifying the lawyer if the provider is served with process requiring the production of client information; (2) investigating the provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances; (3) ensuring the provider uses available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and (4) investigating the provider's ability to purge and wipe any copies of the data, and to move

---

72. Memorandum from the A.B.A. Comm. on Ethics 20/20 Working Group on the Implications of New Technologies 5 (Sept. 20, 2010), https://www.legalethicstexas.com/getattachment/e3d3e98b-fe51-4c4a-9af9-da7bed148d30/Ethics-20-20-Working-Group-Report-on-Electronic-Co.aspx [hereinafter Memo from Ethics 20/20 Re: Technology].

73. *Id*.

74. *E.g*., *Opinion No. 99-03*, 1999 ST. B. ASSOC. OF N.D. ETHICS COMM. 3, https://www.sband.org/userfiles/files/pdfs/ethics/99-03.pdf (determining an online data backup service was appropriate provided the law firm ensured "the security of the data transmission and the security of the data storage are adequate for the sensitivity of the records that are to be transmitted and stored").

75. These ethics opinions are available on the A.B.A.'s website, https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

76. *E.g*., *Opinion 842*, 2010 N.Y. ST. B. ASSOC. COMM. ON PROF. ETHICS, http://www.nysba.org/CustomTemplates/Content.aspx?id=1499.

77. *Id*.

the data to a different host, if the lawyer becomes dissatisfied with the provider or for other reasons changes providers.[78]

In Pennsylvania, reasonable care in selecting and using a cloud provider may also include whether the provider: (1) explicitly agrees it has no ownership or security interest in the data; (2) includes in its "Terms of Service" an agreement about how confidential client information will be handled; (3) provides the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed; (4) provides a method of retrieving data if the lawyer terminates use of the provider's product, the provider goes out of business, or the service otherwise has a break in continuity; (5) will host the firm's data only within a specified geographic area; and (6) provides the ability for the law firm to get data off of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.[79]

Many of these confidentiality considerations likewise apply when outsourcing non-legal support services, such as IT maintenance of a firm's network server.[80] Written confidentiality agreements are strongly advised in relationships with third parties involving access to and disclosure of client information.[81]

IV. THE TECHNOLOGIES LAWYERS ARE USING

It is now an ethical mandate in North Dakota that competent lawyers must be reasonably informed about relevant technology.[82] The types of technology that lawyers are using include local technology and cloud-based technology.[83]

Local technology refers to technology controlled by lawyers and their employees, which includes primary computers,[84] home computers, operating systems,[85] law firm servers, mobile devices, such as laptops,

78. *Id*. at 4. Lawyers should also periodically reconfirm that the provider's security measures remain effective in light of advances in technology. *Id*.

79. *Formal Opinion 2011-200*, 2011 PA. B. ASSOC. COMM. ON LEGAL ETHICS & PROF. RESP. 9, http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

80. *E.g*., *Formal Opinion 08-451*, 2008 A.B.A. COMM. ON ETHICS & PROF. RESP. 5, http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/ethicsopinion08451.authcheckdam.pdf.32.

81. *Id*.

82. N.D. RULES OF PROF'L. CONDUCT r.1.1 (2015).

83. The examples of the types of technology are based on the A.B.A. TechReport 2015, http://www.americanbar.org/publications/techreport/2015.html. Discussion of lawyer technology does not include web-based technology, such as law firm websites and blogs.

84. Meaning desktops and laptops.

85. Such as Windows 8.

smartphones and tablets, printers, scanners, copiers, external hard drives, external media,[86] and email.[87]

Cloud-based technology refers to technology controlled by third parties and accessed over the Internet.[88] Examples of cloud-based technology include third-party servers, Software as a Service ("SaaS"),[89] online data storage (e.g., Dropbox), internet-based email (e.g., Gmail), and instant messaging (e.g., Google Chat).[90]

Lawyers and law firms also use software. Some of the software used may be the traditional model, in which the software is purchased per license and then installed on the computer or network.[91] Alternatively, the software may be the newer model, SaaS, in which the software is not installed on an individual computer or server, but is instead accessed over the Internet and is sold on a subscription basis.[92]

All of this use of technology increases the risk that electronically maintained client information will be impermissibly used, disclosed, stolen, or lost.[93] Risks associated with the use of local technology include: inadequate physical protection for mobile devices or not having the ability to remotely wipe mobile devices that are lost or stolen; weak passwords; failing to purge data from devices before they are replaced (e.g., copiers with scanners); infrequent data backups; not encrypting sensitive information; using unsupported computer operating systems or not having basic security tools such as virus or spyware protection; and using public wifi hotspots when transmitting confidential information. [94]

---

86. Including portable storage devices such as USB drives and flash drives.

87. *Id*.

88. *Id*.

89. SaaS is software that is not installed on an individual computer or server, but is instead accessed over the Internet and is sold on a subscription basis, usually for a monthly fee. A.B.A. TechReport 2015, http://www.americanbar.org/publications/techreport/2015.html.

90. *Id*.

91. *Id*.

92. *Id*. Examples of software (traditional and SaaS) include contact management (e.g., Outlook), remote access (e.g., Citrix), electronic fax (e.g., eFax), voice recognition (e.g., Dragon Natural Speaking), document software for PDF creation (e.g., Adobe), redlining (e.g., Microsoft Word), document management (e.g., NetDocuments), and document assembly (e.g., Hot Docs), software for word processing (e.g., Microsoft Word), calendaring (e.g., Outlook), spreadsheets (e.g., Microsoft Excel), time and billing (e.g., Tabs), trial presentation (e.g., Trial Director), accounting (e.g., Quickbooks), databases (e.g., Filemaker Pro), electronic billing, and image scanners (e.g., Adobe Acrobat), and legal-specific software such as case/practice management (e.g., Clio), conflict checking (e.g., PC Law), security (e.g., Kaspersky antivirus), and encryption (e.g., Outlook). A.B.A. TechReport 2015, http://www.americanbar.org/publications/techreport/2015.html.

93. *Ethics 20/20 Introduction and Overview*, *supra*, note 4, at 1-13.

94. Memo from Ethics 20/20 Re: Technology, *supra* note 72, at 2-6.

Risks associated with the use of cloud computing and outsourcing technology include: inadequate access and authorization controls; the storage of information on servers outside the United States; infrequent or inadequate data backups; insufficient data encryption; unclear or nonexistent vendor policies regarding ownership of stored data or data destruction when the services are terminated; and inadequate or nonexistent vendor policies addressing the handling and safeguarding of confidential information.[95]

Lawyers most certainly understand that there are risks associated with technology and they are paying increased attention to security. According to the A.B.A. TechReport 2015, however, more security measures need to be taken, particularly in light of the frequent headline reports of data breaches.[96] Increasingly, lawyers and law firms are the targets of hackers.[97] It has been reported that since 2011, at least eighty percent of the largest law firms have been hacked.[98] Small and medium firms, too, are targets. Most data breaches involve 10,000 or fewer records and are not mega breaches involving 100,000 or more records.[99] According to the Ponemon Institute's 2016 data breach study, the average total cost of a data breach in the United States is approximately $7.01 million, or $221 per lost or stolen record.[100] Malicious or criminal attacks, such as malware, phishing, and social engineering, are most often the cause of a data breach in the United States, representing forty-nine percent of incidents.[101] Nineteen percent of data breaches are caused by human error, such as a negligent employee or contractor.[102] The remaining thirty-two percent of data breaches involve system glitches which include IT and business process failures.[103]

Law firms are targeted by hackers because of the sensitive and valuable information entrusted to them by their clients and because there is a perception that law firms' security defenses may be weak.[104] There is support for this perception in the A.B.A. 2015 Legal Technology Survey Report that explored which security measures reporting lawyers use.[105]

---

95. *Id*.
96. Reis, *Security*, *supra* note 6, at 1.
97. *Id*.
98. *Id*.
99. *2016 Cost of Data Breach Study: Global Analysis*, 2016 PONEMON INST. 1, https://nhlearningsolutions.com/Portals/0/Documents/2016-Cost-of-Data-Breach-Study.PDF.
100. *Id*. at 2. The cost increases if health care or education records are involved. *Id*.
101. *Id*.
102. *Id*.
103. *Id*.
104. Sedona Conference, *Guidelines for Lawyers*, *supra* note 12, at B-1.
105. Reis, *Security*, *supra* note 6, at 1.

When asked about technology-related policies, fifty-five percent of lawyers reported their firms have a document management and retention policy, but fewer than fifty percent have policies addressing topics like email and Internet use, acceptable use, social media, and employee privacy.[106] In addition, twenty-five percent of firms reported having no security related policies.[107] Only fifty-five percent of firms have an incident response plan, and most do not have a disaster recovery or business continuity plan.[108] Twenty percent of firms reported having had a full security assessment done by an independent third party.[109] Only thirty-eight percent of lawyers felt that security awareness and technology training were very important.[110] Over twenty-three percent of lawyers were unaware of whether their firm had experienced a data breach.[111] Additionally, the use of encryption by lawyers remains low. Overall use of full drive encryption was reported at only twenty percent.[112] Lawyers' use of file encryption was reported to be forty-two percent, and email encryption was reported to be thirty-five percent.[113] The A.B.A. and state bar associations, including North Dakota, have considered the issue of email encryption and generally do not require lawyers to encrypt email communications containing confidential client information under ordinary circumstances.[114] Special circumstances, however, such as transmission of highly sensitive information, can require a lawyer to take additional precautions.[115] These safeguards include

106. *Id*. at 3.

107. *Id*. at 4.

108. *Id*.

109. *Id*.

110. Adriana Linares, *Technology Training*, A.B.A TechReport 2015, at 1, http://www.americanbar.org/content/dam/aba/publications/techreport/2015/training/Training.authcheckdam.pdf.

111. Reis, *Security*, *supra* note 6, at 3; *see also* https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

112. *Id*. at 5-6. Full drive encryption is encryption built into the hard drive of the device by the manufacturer. David G. Ries & John W. Simek, *Encryption Made Simple for Lawyers*, *in* 29 G.P. SOLO MAGAZINE 6, NOVEMBER/DECEMBER 2012: PRIVACY AND CONFIDENTIALITY, http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html.

113. *Id*.

114. *See Formal Opinion 99-413*, 1999 A.B.A. COMM. ON ETHICS & PROF. RESP.; *Formal Opinion 11-459*, 2011 A.B.A. COMM. ON ETHICS & PROF. RESP.; *Opinion No. 97*-09, 1997 STATE BAR ASS'N OF N.D. ETHICS COMM. 7; *see also Opinion No. 2010-179,* 2010 CAL. FORMAL ETHICS (collecting ethics opinions).

115. *Opinion No. 97-09*, 1997 STATE BAR ASS'N OF N.D. ETHICS COMM. 7 (encrypted email is not required "unless unusual circumstances require enhanced security measures"); *Formal Opinion 99-413*, 1999 A.B.A. COMM. ON ETHICS & PROF. RESP. (particularly strong measures would be warranted with disclosures of highly sensitive information).

encryption, the avoidance of email, or a special security request made by a client that might otherwise not be required.[116]

Of the thirty-one percent of lawyers who reported using cloud technology, forty percent used at least one security measure, such as local data backup, but sixteen percent reported using no security measures.[117] Lawyers and law firms fared much better in the area of basic security tools. Ninety-seven percent required authentication and access controls for networks, computers, and mobile devices.[118] Regarding critical security tools, eighty-seven percent used spam filters, seventy-eight percent used anti-spyware software, and seventy-nine percent used software-based firewalls.[119] Twenty-two percent reported the use of intrusion detection and prevention systems.[120] Over ninety-nine percent of reporting lawyers and law firms backup their systems, most on a daily basis.[121]

Lawyers need to improve these numbers, as a matter of legal and professional responsibility and client service. Clients are increasingly insisting on sound and strict information security practices from their lawyers.[122] On cyberinsurance applications, cybersecurity insurance carriers, too, are asking law firms about their information security practices. Some law firms are obtaining cybersecurity industry certification to demonstrate their commitment to security,[123] such as the ISO 27001 certification, an international standard promulgated by the International Organization for Standardization (ISO).[124] This certification requires implementing and adhering to a comprehensive set of security management protocols.[125]

---

116. *See* N.D. RULES OF PROF'L CONDUCT r.1.6 cmt. 18 (2015).

117. Dennis Kennedy, *Cloud Computing*, A.B.A. TechReport 2015, at 2, http://www.americanbar.org/content/dam/aba/publications/techreport/2015/cloud-computing/Cloud-Computing.authcheckdam.pdf.

118. Reis, *Security*, *supra* note 6, at 5-6.

119. *Id*.

120. *Id*. at 5.

121. *Id*. at 7.

122. Sedona Conference, *Guidelines for Lawyers*, *supra* note 12, at B-2.

123. *E.g*., Joseph D. Cohen & Jonathan L. Schwartz, *Should Law Firms Be Concerned about Cyberattacks?: Is Cybersecurity Certification Right for Your Law Firm?* 57 No. 10 DRI FOR THE DEFENSE 18 (2015).

124. *Id*.

125. *Id*. at 19.

V. LAWYERS AND LAW FIRMS MUST SECURE THEIR INFORMATION SYSTEMS

In August 2014, two years after approving the Technology Amendments, the A.B.A. adopted the recommendation of the ABA Cybersecurity Legal Task Force, which encouraged all private and public sector organizations, including law firms, "to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected."[126] It is a recommendation consistent with the A.B.A.'s ongoing efforts to educate and provide guidance to lawyers about their information security obligations.[127]

In North Dakota, "applicable ethical obligations" now require lawyers act competently to safeguard client information by making reasonable efforts to secure information systems and prevent the impermissible access to or disclosure of client information.[128] Rule 1.6 does not tell lawyers what constitutes reasonable efforts or what safeguards or security measures to implement. What measures should be implemented will depend on the information to be protected and secured based on an assessment of the new factors under Comment [18]. Highly sensitive information, for example, will require heightened security safeguards.[129] What is reasonable will change as technology changes.

The Comment [18] factors allow for flexibility and practicality in the ways in which lawyers approach their obligation to secure their information systems. Lawyers should consider more formal, preferably written, information security or cybersecurity programs.[130] For those lawyers with health care and financial services clients, comprehensive written information security programs are already a legal obligation; therefore, these lawyers are not likely presented with new challenges in satisfying

126. *Resolution 109*, *supra* note 61.

127. The ABA Cybersecurity Legal Task Force was created in 2009 by then-A.B.A. President Laurel Bellows. Its mission is to "identify and compile resources within the ABA that pertain to cybersecurity, and [to] focus and coordinate the ABA's legal and policy analyses and assessments of proposals relating to cybersecurity." http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aboutcyber.html.

128. *Id*.; N.D. RULES OF PROF'L. CONDUCT r.1.6 (2015).

129. N.D. RULES OF PROF'L. CONDUCT r .1.6 cmt. 18 (2015).

130. Lucy L. Thomson & Randy V. Sabett, *Understanding Cyber and Data Security Risks and Best Practices*, *in ABA Cybersecurity Handbook*, *supra* note 29, at 7 (discussing the obligation of lawyers to implement data security programs).

their ethical obligation.[131] For other lawyers, now is the time to undertake the task of developing and implementing an information security program which is customized to both the scope and nature of the law firm practice, as well as the type of systems and data that will be protected.[132]

The goal of any information security program is to ensure the confidentiality, availability, and integrity of information.[133] Confidentiality means that private and confidential information is accessible only to those who need to use it.[134] Availability means the information is accessible when needed.[135] Integrity means the information is not corrupted or altered.[136] There is a wealth of resources available to lawyers that provides guidance about information security programs.[137]

In addition to publicly available cybersecurity resources,[138] some of which are industry-specific[139] and some which are generally applicable,

---

131. *E.g.*, 45 C.F.R. § 160.103 (2016) (defining "business associate" to include a person who provides legal services to a covered entity).

132. *Resolution 109*, *supra* note 61, at 1; David G. Ries, *Cyber Security for Attorneys: Understanding the Ethical Obligations*, L. PRAC. TODAY, at 4 (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/cyber-security-for-attorneys-understanding-the-ethical-obligations.authcheckdam.pdf.

133. *ABA Cybersecurity Handbook*, *supra* note 29, at 39; *e.g.*, 44 U.S.C. § 35423552(b)(3) (2016).

134. Sedona Conference, *Guidelines for Lawyers*, *supra* note 12, at 4; *see also* 42 C.F.R. § 164.306(a)(1) (requiring covered entities and business associates "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information").

135. *Id.*

136. *Id.*

137. *Infra* notes 137-139. As explained by the A.B.A. Cybersecurity Legal Task Force:

> A cybersecurity program is comprised of a series of activities. These activities include, for example: governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training.
>
> [C]ertain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can provide early detection of threats.
>
> Privacy compliance requirements should be incorporated into the cybersecurity program. In addition, an effective cybersecurity program requires trained personnel. . . .
>
> Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets.

Resolution 109, *supra* note 61, at 6.

138. For public resources, see *Small Business Information Security: The Fundamentals*, 7621 NAT'L INST. OF STANDARDS & TECH (2014), http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf; *see also Best Practices for Victim Response and Reporting of Cyber Incidents*, U.S. DEP'T OF JUST. CYBERSECURITY UNIT (2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf; *see also Start With Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also* COMMONWEALTH OF MASSACHUSETTS, OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, *201 CMR 17.00 Compliance Checklist*, http://www.mass.gov/ocabr/docs/

more lawyer-specific resources are becoming available.[140] Two legal resources that are invaluable to lawyers are the *ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*[141] and the Sedona Conference's recent publication, *Commentary on Privacy and Information Security Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*.[142]

Developing an information security program is not one-size-fits-all. There are different approaches and no uniform standard among the available resources.[143] To get started, lawyers should develop and maintain knowledge of applicable ethical, legal, and contractual obligations that govern client information entrusted to their care. Different laws govern different types of information, and, therefore, may require different levels of protection depending on, among other things, the nature of the information, the circumstances in which the information is held, and how it is used and disclosed.[144]

---

idtheft/compliance-checklist.pdf; *see also Cybersecurity Risk Management: A Non-Technical Guide, Essential for Business Managers Officer Managers Operations Managers*, 2012 NYS OFFICE OF CYBERSECURITY, https://www.its.ny.gov/sites/default/files/documents/Risk-Management-Guide-2012.pdf; *see also* SANS, *CIS Critical Security Controls for Effective Cyber Defense*, https://www.sans.org/critical-security-controls.

139. For industry-specific resources, see *Guide to Privacy and Security of Electronic Health Information*, NAT'L COORDINATOR FOR HEALTH INFO. TECH. (Apr. 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf; *see also Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying; *see also Cyberplanner*, FED. COMM. COMM'N, https://www.fcc.gov/cyberplanner (last visited July 5, 2016); *see also Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.1*, PCI SECURITY STANDARDS COUNCIL (Apr. 2015), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

140. For lawyer-specific resources, see *Legal Tech. Resource Ctr.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources (last visited July 5, 2016); *see also ABA Cybersecurity Legal Task Force,* A.B.A., http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity (last visited July 5, 2016); *see also* Sedona Conference, *Guidelines for Lawyers*, *supra* note 12; *see also* ethics opinions of the A.B.A. and state bar associations addressing lawyers' use of technology, cloud computing, email and electronic communications, and metadata, which are available on the A.B.A. website that maintains many ethics opinions. *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited July 5, 2016).

141. *ABA Cybersecurity Handbook*, *supra* note 29.

142. Sedona Conference, *Guidelines for Lawyers*, *supra*, note 12.

143. A comprehensive discussion of all the components of an information security program is beyond the scope of this Article. Resources have been suggested that will provide guidance for lawyers and law firms about developing, implementing and maintaining a reasonable and appropriate information security program. *Supra* notes 13, 29, 139-41.

144. For example, HIPAA applies to protected health information, paper and electronic. 45 C.F.R. § 160.103. North Dakota State Breach Notification Law applies to a breach of electronic data that includes personal information. N.D. CENT. CODE § 51-30-01(1) (2015). New Rule

To determine which measures should be taken to protect and secure client information, it will be necessary to perform a risk assessment that includes identifying what information is maintained, and where and how it is stored, transmitted, used and disclosed; classifying the information based on its sensitivity and risk if it was impermissibly accessed or disclosed; and identifying and inventorying all information systems that house data and information.[145] Based on the risk assessment, well thought-out security measures and practices can be developed and formalized in policies that address administrative, technical, and physical safeguards.[146] Administrative safeguards are the administrative actions, policies, and other documentation that will guide the conduct of lawyers and non-lawyers within the firm.[147] Technical safeguards are the IT protocols and policies that control use of and access to information systems.[148] Physical safeguards are the physical measures and policies that protect and control access to information systems, buildings, and equipment.[149] To ensure

---

1.6(d) applies to "information relating to the representation of a client." N.D. RULES OF PROF'L CONDUCT r.1.6(d). Consideration should be given to choosing a security framework with which to align the program. There are regulatory and voluntary industry standards. An example of a regulatory security standard is HIPAA's Security Rule. 45 C.F.R. Part 164, subp. A, C (2016); 45 C.F.R. § 164.306 (2016). Voluntary standards include NIST's Framework for Improving Critical Infrastructure Cybersecurity and ISO's 27000 series. *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; *See NIST Cybersecurity Framework Core: Informative Reference Standards*, A.B.A. (Apr. 2014), http://www.americanbar.org/content/dam/aba/administrative/law_national_security/nistframework/NIST%20Cybersecurity%20Framework%20Core%20-%20ISO-IEC%2027001.authcheckdam.PDF.

145. *Guide for Conducting Risk Assessments*, 800-30 NIST 5 (2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (example of a risk assessment approach and methodology); 45 C.F.R. Part 164, Subparts A, C (2016) (setting forth the required standards and implementation specifications of HIPAA's Security Rule); *ABA Cybersecurity Handbook*, *supra* note 29, at ch. 4 (discussing cybersecurity programs for law firms).

146. *E.g.*, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, 800-37 NIST F-10 (Feb. 2010), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf (shown as an example of how to apply a risk management framework). Written policies should address, at a minimum, information access and authentication controls; physical security; network security; encryption; Internet, email, electronic communication and social media usage; mobile security, remote access and personal devices; equipment and media reuse, sanitization, and disposal; secure backup of information; document retention and destruction; and litigation holds and preservation of evidence. *See*, *e.g.*, 45 C.F.R. Part 164, Subparts A, C (setting forth the required standards and implementation specifications of HIPAA's Security Rule). North Dakota has an ethics opinion addressing the record retention obligations of lawyers for client files and storing them electronically. *Opinion No. 11*-03, STATE BAR ASS'N. OF N.D.

147. *See, e.g.*, 45 C.F.R. § 164.304 (2016).

148. *Id.*

149. *Id.* An information security program should also include a plan for responding to and recovering from incidents involving an impermissible use or disclosure, theft or loss of client information. *See* 45 C.F.R. § 164.308(a)(6) (2016). An incident response plan will provide an organized approach for handling threats to information systems and data, and for taking action if a breach occurs. Tracy Vigness Kolb, *Anatomy of an Incident Response and Data Breach—How*

compliance with the information security program, regular education and security awareness training of the entire workforce should be provided and ongoing oversight and monitoring activities should be conducted.[150]

An information security program should also address the handling and safeguarding of client information entrusted to others outside of the firm.[151] At a minimum, contracts should be in place that require confidentiality and address how the information will be handled and safeguarded.[152] It makes no sense to secure one's own information system only to provide client information to others without knowing the security of their systems.

Perfect protection and security of client information is not possible or required;[153] and lawyers are not required under the new ethical obligations to be, or become, technology experts. The rules do contemplate, however, that lawyers recognize if they have technology limitations and obtain appropriate expertise if necessary.[154]

VI. CONCLUSION

The ethical rules have long imposed professional obligations on lawyers to protect client information. Our digital world, however, has transformed the legal profession, creating unique and challenging issues for lawyers because of the growing significance of technology on modern law practice. Lawyers are using technology and, therefore, need to understand and stay informed about technology to provide competent representation to clients and to understand its impact on all aspects of law practice. This is particularly so with respect to privileged and confidential client information.

Lawyers Can Plan and Prepare, State Bar Association of North Dakota, 2016 Annual Convention (June 16, 2016). A business continuity and disaster recovery plan will help prepare in advance for recovering from cyber events and disruptions to business operations. *E.g.*, *Computer Security Incident Handling Guide*, 800-61 NIST (Aug. 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf; *Contingency Planning Guide for Federal Information Systems*, 800-34 NIST (May 2010), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf. ISO has two standards, ISO 22301 (Business continuity management systems) and ISO 27031 (Information and communications technology readiness for business continuity). *ISO 22301:2012*, ISO, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038 (last visited July 5, 2016); *ISO/IEC 27031:2011*, ISO, http://www.iso.org/iso/catalogue_detail.htm?csnumber=44374 (last visited July 5, 2016).

150. *E.g.*, 45 C.F.R. §§ 164.308(a)(5), 164.312(b) (2016). Training may also include security awareness efforts such as security tips and reminders. *Id.* Monitoring activities should include network and user activity log analysis, audits, penetration testing, and annual independent IT security audits or reviews. *Id.; see also ABA Cybersecurity Handbook*, *supra* note 29, at ch. 4 (discussing cybersecurity programs for law firms).

151. *See, e.g.*, 45 C.F.R. §§ 164.502(e)(2), -.314(a)(1) (2016).

152. *Id.;* Memo from Ethics 20/20 Re: Technology, *supra* note 72.

153. *Ethics 20/20 Introduction and Overview*, *supra* note 4, at 8.

154. MODEL RULES OF PROF'L CONDUCT r.1.1 cmt. 8 (2013).

Lawyers and law firms are "information fiduciaries."[155] Now grounded in the ethics rules is a lawyer's duty to protect and secure client confidences. Lawyers should continue to increase their level of technology competence in order to effectively address the risks and threats to the security of their information systems and should make reasonable efforts to secure those systems, including developing and implementing an information security program.

Not doing so may result in a breach of the very essence of the attorney-client relationship—the obligation to ensure client confidences are protected and the attorney-client privilege is preserved.

155. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 204-05 (2015).