

1 **Securing Communication of Protected Client Information**

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

9

10 I. Introduction

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

15 Formal Opinion 99-413 concluded: “Lawyers have a reasonable expectation of privacy in
16 communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet,
17 despite some risk of interception and disclosure. It therefore follows that its use is consistent with
18 the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information
19 relating to a client’s representation.”¹

20 Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers
21 primarily use electronic means to communicate and exchange documents with clients, other
22 lawyers, and even with other persons who are assisting a lawyer in delivering legal services to
23 clients.²

24 Since 1999, those providing legal services now regularly use a variety of devices to create, transmit
25 and store confidential communications, including desktop, laptop and notebook computers, tablet
26 devices, smartphones, and cloud resource and storage locations. Each device and each storage
27 location offer an opportunity for the inadvertent or unauthorized disclosure of information relating
28 to the representation, and thus implicate a lawyer’s ethical duties.³

¹ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 99-413, at 11 (1999).

² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

³ See JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

29 In 2012 the ABA adopted “technology amendments” to the Model Rules, including updating the
30 Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new
31 Comment to Rule 1.6, addressing a lawyer’s obligation to take reasonable measures to prevent
32 inadvertent or unauthorized disclosure of information relating to the representation.
33

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

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

45 Against this backdrop we describe the “technology amendments” made to the Model Rules in
46 2012, identify some of the technology risks lawyers’ face, and discuss factors other than the Model
47 Rules of Professional Conduct that lawyers should consider when using electronic means to
48 communicate regarding client matters.

49 II. Duty of Competence

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

⁴ “Cybersecurity” is defined as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” CYBERSECURITY, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/cybersecurity> (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

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

⁶ A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

56 To maintain the requisite knowledge and skill, a lawyer should keep abreast of
57 changes in the law and its practice, including the benefits and risks associated with
58 relevant technology, engage in continuing study and education and comply with all
59 continuing legal education requirements to which the lawyer is subject. (Emphasis
60 added.)⁷

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

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

70 III. Duty of Confidentiality

71 In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts
72 are required to preserve the confidentiality of information relating to the representation. Model
73 Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a
74 client" unless certain circumstances arise.⁹ The 2012 modification added a new duty in paragraph
75 (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized
76 disclosure of, or unauthorized access to, information relating to the representation of a client."¹⁰

77 Amended Comment [18] explains:

78 Paragraph (c) requires a lawyer to act competently to safeguard information relating
79 to the representation of a client against unauthorized access by third parties and
80 against inadvertent or unauthorized disclosure by the lawyer or other persons who
81 are participating in the representation of the client or who are subject to the lawyer's

⁷ *Id.* at 43.

⁸ ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_a_mended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

⁹ MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

¹⁰ *Id.* at (c).

82 supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the
83 inadvertent or unauthorized disclosure of, information relating to the representation
84 of a client does not constitute a violation of paragraph (c) if the lawyer has made
85 reasonable efforts to prevent the access or disclosure.

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

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

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

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

- 108 (1) The sensitivity of the information,
- 109 (2) The likelihood of disclosure if additional safeguards are not employed,
- 110 (3) The cost of employing additional safeguards,
- 111 (4) The difficulty of implementing the safeguards, and

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

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

112 (5) The extent to which the safeguards adversely affect the lawyer’s ability to represent
113 clients (e.g., by making a device or important piece of software excessively difficult
114 to use).¹³
115

116 A fact-based analysis means that particularly strong protective measures, like encryption, are
117 warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security
118 safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed
119 consent from the client regarding whether to the use enhanced security measures, the costs
120 involved, and the impact of those costs on the expense of the representation where nonstandard
121 and not easily available or affordable security methods may be required or requested by the client.
122 Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding
123 the use of electronic methods or any technology to communicate with the client altogether, just as
124 it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.
125

126 In contrast, for matters of normal or low sensitivity, standard security methods with low to
127 reasonable costs to implement, may be sufficient to meet the reasonable efforts standard to protect
128 client information from inadvertent and unauthorized disclosure.
129

130 In the technological landscape of Opinion 99-413, and due to the reasonable-expectations of
131 privacy available to email communications at the time, unencrypted email posed no greater risk of
132 interception or disclosure than other non-electronic forms of communication. This basic premise
133 remains true today for routine communication with clients, presuming the lawyer has implemented
134 basic and reasonably available methods of common electronic security measures.¹⁴ Thus, the use
135 of unencrypted routine email generally remains an acceptable method of lawyer-client
136 communication.
137

138 However, cyber-threats and the proliferation of electronic communications devices have changed
139 the landscape and it is not always reasonable to rely on the use of unencrypted email. For example,
140 electronic communication through certain mobile applications or on message boards or via
141 unsecured networks may lack the basic expectation of privacy afforded to email communications.
142 Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate
143 electronically about client matters, applying the Comment [18] factors to determine what effort is
144 reasonable.
145

¹³ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2013). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

¹⁴ See item 3 below.

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

148

149 1. Understand the Nature of the Threat.

150

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

157

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

159

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

167

168 3. Understand and Use Reasonable Electronic Security Measures.

169

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

179

180 A lawyer should understand and use electronic security measures to safeguard client
181 communications and information. A lawyer has a variety of options to safeguard
182 communications including, for example, using secure internet access methods to
183 communicate, access and store client information (such as through secure Wi-Fi, the use

¹⁵ See, e.g., Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/>.

184 of a Virtual Private Network, or another secure internet portal), using unique complex
185 passwords, changed periodically, implementing firewalls and anti-Malware/Anti-
186 Spyware/Antivirus software on all devices upon which client confidential information is
187 transmitted or stored, and applying all necessary security patches and updates to
188 operational and communications software. Each of these measures is routinely accessible
189 and reasonably affordable or free. Lawyers may consider refusing access to firm systems
190 to devices failing to comply with these basic methods. It also may be reasonable to use
191 commonly available methods to remotely disable lost or stolen devices, and to destroy the
192 data contained on those devices, especially if encryption is not also being used.

193
194 Other available tools include encryption of data that is physically stored on a device and
195 multi-factor authentication to access firm systems.

196
197 In the electronic world, “delete” usually does not mean information is permanently deleted,
198 and “deleted” data may be subject to recovery. Therefore, a lawyer should consider
199 whether certain data should *ever* be stored in an unencrypted environment, or electronically
200 transmitted at all.

201
202 4. Determine How Electronic Communications About Clients Matters Should Be Protected.

203
204 Different communications require different levels of protection. At the beginning of the
205 client/lawyer relationship, the lawyer and client should discuss what levels of security will
206 be necessary for each electronic communication about client matters. Communications to
207 third parties containing protected client information requires analysis to determine what
208 degree of protection is appropriate. In situations where the communication (and any
209 attachments) are sensitive or warrant extra security, additional electronic protection may
210 be required. For example, if client information is of sufficient sensitivity, a lawyer should
211 encrypt the transmission and determine how to do so to sufficiently protect it,¹⁶ and
212 consider the use of password protection for any attachments. Alternatively, lawyers can
213 consider the use of a well vetted and secure third-party cloud based file storage system to
214 exchange documents normally attached to emails.

215
216 Thus, routine communications sent electronically are those communications that do not
217 contain information warranting additional security measures beyond basic methods.
218 However, in some circumstances, a client’s lack of technological sophistication or the
219 limitations of technology available to the client may require alternative non-electronic
220 forms of communication altogether.

¹⁶ See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59

221
222 A lawyer also should be cautious in communicating with a client if the client uses
223 computers or other devices subject to the access or control of a third party.¹⁷ If so, the
224 attorney-client privilege and confidentiality of communications and attached documents
225 may be waived, and the lawyer must determine whether it is prudent to warn a client of the
226 dangers associated with such a method of communication.¹⁸

227
228 5. Label Client Confidential Information.

229
230 Lawyers should follow the better practice of marking privileged and confidential client
231 communications as “privileged and confidential” in order to alert anyone to whom the
232 communication was inadvertently disclosed that the communication is intended to be
233 privileged and confidential. This can also consist of something as simple as appending a
234 message or “disclaimer” to client emails, where such a disclaimer is accurate and
235 appropriate for the communication.¹⁹

236
237 Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has
238 received an inadvertently sent “document or electronically stored information relating to
239 the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear
240 and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s
241 duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

¹⁷ See, e.g., ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect the confidentiality of e-mail communications with one’s client); Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer’s email server).

¹⁸ Some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, See, e.g., Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer...;
4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

¹⁹ See Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280

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

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

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

7. Conduct Due Diligence on Vendors Providing Communication Technology.

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

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

- a. Reference Checks and Vendor Credentials
- b. Vendor’s Security Policies and Protocols

- 281 c. Vendor’s Hiring Practices
282 d. The Use of Confidentiality Agreements
283 e. Vendor’s Conflicts Check System to Screen for Adversity
284 f. The Availability and Accessibility of a Legal Forum for Legal Relief for
285 Violations of the Vendor Agreement.

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

289 Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added
290 to address outsourcing, including “using an Internet-based service to store client
291 information.” Comment [3] provides that the “reasonable efforts” required by Model Rule
292 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with
293 the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3]
294 contains suggested factors that might be taken into account:

- 295 • “the education, experience, and reputation of the nonlawyer;
296 • the nature of the services involved;
297 • the terms of any arrangements concerning the protection of client information; and
298 • the legal and ethical environments of the jurisdictions in which the services will be
299 performed particularly with regard to confidentiality.”
300

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

²⁰ MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

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

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

307
308 Even after a lawyer examines these various considerations and is satisfied that the security
309 employed is sufficient to comply with the duty of confidentiality, the lawyer must
310 periodically reassess these factors to confirm that the lawyer’s actions continue to comply
311 with the ethical obligations and have not been rendered inadequate by changes in
312 circumstances or technology.

313 IV. Duty to Communicate

314 Communications between a lawyer and client generally are addressed in Rule 1.4. When the
315 lawyer reasonably believes that highly sensitive confidential client information is being
316 transmitted so that extra measures to protect the email transmission are warranted, the lawyer
317 should inform the client about the risks involved.²³ The lawyer and client then should decide
318 whether another mode of transmission, such as high level encryption or personal delivery is
319 warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely
320 use technology in their communication, in compliance with other laws that might be applicable to
321 the client. Whether a lawyer is using methods and practices to comply with administrative,
322 statutory, or international legal standards is beyond the scope of this opinion.

323 A client may insist or require that the lawyer undertake certain forms of communication. As
324 explained in Comment [18] to Model Rule 1.6, “A client may require the lawyer to implement
325 special security measures not required by this Rule or may give informed consent to the use of a
326 means of communication that would otherwise be prohibited by this Rule.”

327 V. Conclusion.

328 Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule
329 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation,
330 a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule
331 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized
332 disclosure of or access to information relating to the representation.

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

²³ MODEL RULES OF PROF’L CONDUCT R. 1.4(a)(1) & (4) (2016).