

To: COPRAC  
From: Dena Roche  
Re: 16-0002 Data Breaches (Post-Public Comment)

---

I have reviewed all the public comments on the Data Breach opinion, and attached is a suggested redline version incorporating many of those comments into the draft. I did not include all suggested revisions, and am open to discussion on any I did not include, or ones I proposed adding through the attached redline.

Among those I did not include are:

Duties to Former Clients: Two of the comments suggested including a section on duties to former clients. In drafting this opinion, we took the approach that the ABA took in Formal Opinion 483, which is since there is nothing in the rules requiring notice to a former client as a matter of legal ethics we would not impose such a duty. Yes, there are duties to former clients not to use or reveal confidential information (rule 1.9), but how would we resolve the issue of notice?

LACBA Nos. 8-10: LACBA raised several questions about defining data breach for the purposes of the opinion and the scope of when notice is appropriate to clients. We intentionally defined data breach broadly, using the ABA definition, for uniformity purposes and because we felt it was broad enough to encompass all types of scenarios in which data is compromised. I agree with our guidance on notice, but I am interested in how others feel about those comments.

LACBA No 4: LACBA suggested that there should be language clarifying that lawyers are not expected to be experts in technology and can reasonably rely on IT consultants to meet their ethical obligations. Do we want to/need to cite to the other opinions to include this concept?

Confidentiality and Duty of Competence: Should we include a comment in this section that rule 1.1 does not have a comment 8 (like ABA rules re technology competence), or provide an update on the status of change in rules and recommendations to include such a comment in the California rules?

Further Analysis of 2010 Opinion as Applied to Attorney D Facts: OCBA suggested that we analyze our facts for Attorney D and whether given our 2010 opinion, there was a per se violation, and if not, what are steps a lawyer should take before using a public network. Thoughts?

1 THE STATE BAR OF CALIFORNIA  
2 STANDING COMMITTEE ON  
3 PROFESSIONAL RESPONSIBILITY AND CONDUCT  
4 FORMAL OPINION INTERIM NO. 16-0002

5 **ISSUE:** What are a lawyer’s ethical obligations with respect to unauthorized  
6 access by third persons to electronically stored ~~client~~-confidential [client](#)  
7 information in the lawyer’s possession?

8 **DIGEST:** Lawyers who use electronic devices which contain confidential client  
9 information must assess the risks of keeping such data on electronic  
10 devices and computers, and take reasonable steps to secure their  
11 electronic systems to minimize the risk of unauthorized access. In the  
12 event of a breach, lawyers have an obligation to conduct a reasonable  
13 inquiry to determine the extent and consequences of the breach and to  
14 notify any client whose interests have a reasonable possibility of being  
15 negatively impacted by the breach.

16 **AUTHORITIES**

17 **INTERPRETED:** Rules 1.1, 1.4, 1.6, 5.1, 5.2, and 5.3 of the Rules of Professional Conduct  
18 of the State Bar of California.<sup>1</sup>

19 Business and Professions Code sections 6068(e) and 6068(m).

20 Civil Code section 1798.82.

21 **INTRODUCTION**

22 Data breaches resulting from lost, stolen or hacked electronic devices and systems are a reality  
23 in today’s world. There are important ethical concerns when data breaches happen to lawyers  
24 and law firms since such events may involve the potential loss of, or unauthorized access to,  
25 confidential client information<sup>2</sup> and, thus, may require a lawyer to take certain remedial steps  
26 to protect the client.

27 In Cal. State Bar Formal Opn. No. 2015-193, the Committee on Professional Responsibility and  
28 Conduct (“COPRAC” or “Committee”) discussed lawyers’ ethical obligations when dealing with  
29 e-discovery. In Cal. State Bar Formal Opn. No. 2010-179, the Committee discussed ethical issues

---

<sup>1</sup> Unless otherwise indicated, all references to “rules” in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

<sup>2</sup> [The phrase “confidential client information” in this opinion includes not only attorney-client privileged communications, but more broadly all client information protected from disclosure under Business and Profession Code section 6068\(e\)\(1\) and rule 1.6.](#)

30 ~~arising from accessing~~that arise when a lawyer accesses ~~client~~ confidential client information on  
31 a laptop over public Wi-Fi ~~and or~~ a home Wi-Fi network. In both opinions, the Committee  
32 adopted an approach that posed questions lawyers should consider in order to comply with the  
33 duties of competence~~y~~ and confidentiality. In light of ever changing technology, the Committee  
34 concluded~~s~~ that an on-going engagement with that evolving technology in the form of security  
35 issues to consider and re-consider was preferable to a “bright line” or categorical approach.

36 This opinion extends that analysis to a broad range of cyber risks associated with the use of  
37 electronic devices and systems that contain ~~client~~ confidential client information and connect  
38 to the internet and, thus, are theoretically accessible to anyone with an internet connection.

## 39 **STATEMENT OF FACTS**

### 40 **Attorney A**

41 Attorney A’s laptop is stolen. Attorney A did not store confidential client information on the  
42 laptop, but only used the laptop to access such information remotely. Also, the laptop could  
43 not be accessed without biometric authentication. Attorney A’s law firm also installed software  
44 on the laptop that allowed it to be remotely locked down and erased. As soon as Attorney A  
45 realizes that the laptop has been stolen, Attorney A contacts law firm’s IT department and  
46 receives confirmation almost immediately that the laptop has been located, locked down and  
47 wiped clean.

### 48 **Attorney B**

49 At the end of a busy day, Attorney B realized that Attorney has lost Attorney’s smartphone.  
50 Attorney B regularly uses the smartphone to email and text clients and to access certain  
51 practice management software applications related to clients. The smartphone is protected  
52 only by a 4-character password and not any biometric data. Attorney B does not have any  
53 software installed on the smartphone that allows it to be remotely tracked, locked down  
54 and/or wiped clean.

55 Before going to bed, Attorney B remembers that Attorney left the smartphone in a tote bag at  
56 the restaurant where Attorney had dinner with a friend. Attorney B immediately calls the  
57 restaurant, but it is closed. Attorney B goes to the restaurant when it opens the next morning  
58 and retrieves Attorney’s bag and smartphone which, the manager tells Attorney, was locked in  
59 a cabinet overnight. Nothing appears to be missing and the smartphone is still in the pocket of  
60 the bag where Attorney had left it.

### 61 **Law Firm C**

62 Law Firm C is a four-member firm specializing in corporate law. Law Firm’s receptionist  
63 routinely receives e-mails sent to the firm (rather than to a specific attorney or staff member)  
64 and routes them to the appropriate person. Just before quitting time, the receptionist received  
65 an e-mail from a business purporting to be Law Firm’s IT provider; it looked entirely genuine

66 and asked the receptionist to click on the attachment to allow the firm to do routine  
67 maintenance on Law Firm’s server. Receptionist did so and ransomware installed itself on Law  
68 Firm’s network, immediately locked up the Law Firm’s computers, and displayed a message  
69 demanding that a sum of money be transferred electronically by cryptocurrency to unlock Law  
70 Firm’s computers. Law Firm C paid the ransom and regained access to its data. In consultation  
71 with security experts, Law Firm C determined that no client information was accessed and none  
72 of the matters being handled by Law Firm were negatively impacted by the delay.

73 **Attorney D**

74 Attorney D is outside counsel for a life sciences technology company (“Company”) for whom  
75 Attorney has been working on obtaining several very important patents. On vacation, Attorney  
76 D goes to a coffee shop to check personal and work e-mails. Attorney D's laptop was not  
77 encrypted. Instead of using a virtual private network or personal hotspot to connect to the  
78 internet, Attorney accesses the shop’s public Wi-Fi network. Unknown to patrons or coffee  
79 shop staff, a hacker had set up a fake internet portal that resembled the one provided by the  
80 coffee shop. Attorney D doesn’t realize that Attorney actually logged on to that fake network.

81 Attorney D returned to the same coffee shop the next day and noticed a sign warning patrons  
82 about the fake internet portal. Upon return to the office the following week, Attorney D had  
83 the law firm’s technology team examine the laptop. The technology team concluded that  
84 someone had accessed certain files on the laptop related to Company’s patents while Attorney  
85 D had been on the fake internet network. Since Attorney D was not reviewing those files on  
86 that day, it appeared reasonably likely that an unauthorized user had done so.

87 **DISCUSSION**

88 **Confidentiality and Duty of Competence**

89 The duty of competence (rule 1.1) and the duty to safeguard clients’ confidences and secrets  
90 (rule 1.6 and Bus. & Prof. Code, § 6068(e)) require lawyers to make reasonable efforts to  
91 protect such information from unauthorized disclosure or destruction. The threshold  
92 requirement is for lawyers to have a basic understanding of the “benefits and risks associated  
93 with relevant technology.” Cal. State Bar Formal Opn. No. 2015-193. This general principle  
94 requires lawyers to have a basic understanding of the risks posed when using a given  
95 technology and, if necessary, obtain help from appropriate technology experts on assessing  
96 those risks and taking reasonable steps to prevent data breaches which potentially can harm  
97 clients. The threshold obligation to understand the risks is satisfied by learning where and how  
98 confidential [client](#) information is vulnerable to unauthorized access. This inquiry must be made  
99 with respect to each type of electronic device or system as they have been or are incorporated  
100 into the lawyer’s practice.

101 For example, computer systems can be breached by inadvertently clicking on a link in a  
102 seemingly legitimate “phishing” e-mail or text message or by installing an unvetted software  
103 application which can install malicious software on the system. Portable electronic devices can

104 be accessed if security precautions such as passwords are missing or inadequate. Data on  
105 laptop computers can be accessed if the laptop is connected to a public or other inadequately  
106 secured network and if the data is not properly protected. And the threats vary and widen as  
107 data thieves develop their attack strategies and as technologies develop. Thus, lawyers must  
108 understand how their particular use of electronic devices and systems pose risks of  
109 unauthorized access, they must be knowledgeable about the options available at any given  
110 point in time to minimize those risks (including how best to store or control access to said  
111 information), and they then must implement reasonable security measures in light of the risks  
112 posed. In addition, because law firms are frequent targets, law firms should consider [whether](#)  
113 [rule 5.1 requires law firms to ~~preparing~~ prepare](#) a data breach response plan so that all  
114 stakeholders know how to respond when a breach occurs.<sup>3</sup>

115 ABA Formal Opn. No. 18-483 (Lawyer’s Obligations After an Electronic Data Breach or  
116 Cyberattack) provides a useful list of competence-based duties that explain the requirement of  
117 “reasonable efforts” in addressing the potential for inadvertent disclosure of confidential client  
118 information due to a data breach:

- 119 • The obligation to monitor for a data breach: “lawyers must employ reasonable efforts to  
120 monitor the technology and office resources connected to the internet, external data  
121 sources, and external vendors providing services relating to data and the use of data.”  
122 *Id.* at p. 5.
- 123 • When a breach is detected or suspected, lawyers must “act reasonably and promptly to  
124 stop the breach and mitigate damage resulting from the breach.” *Id.* at p. 6. A  
125 preferable approach is to have a data breach plan in place “that will allow the firm to  
126 promptly respond in a coordinated manner to any type of security incident or cyber  
127 intrusion.” *Id.* at p. 6.
- 128 • Investigate and determine what happened: “Just as a lawyer would need to assess  
129 which paper files were stolen from the lawyer’s office, so too lawyers must make  
130 reasonable attempts to determine whether electronic files were accessed, and if so,  
131 which ones. A competent attorney must make reasonable efforts to determine what  
132 occurred during the data breach.” *Id.* at p. 7.

133 The duty to make reasonable efforts to preserve ~~client~~ confidential [client](#) information does not  
134 create a strict liability standard nor does the duty “require the lawyer to be invulnerable or  
135 impenetrable.” ABA Formal Opn. No. 18-483 at p. 9. The precise nature of the security  
136 measures attorneys are expected to take depends on the circumstances. But, as the ABA has  
137 noted, “a legal standard for ‘reasonable’ security is emerging. That standard rejects  
138 requirements for specific security measures (such as firewalls, passwords, or the like) and  
139 instead adopts a fact-specific approach to business security obligations that requires a ‘process’

---

<sup>3</sup> Discussed in ABA Formal Opn. No. 18-483 at pp. 6-7 and in the ABA Cybersecurity Handbook.

140 to assess risks, identify and implement appropriate security measures responsive to those risks,  
141 verify that the measures are effectively implemented, and ensure that they are continually  
142 updated in response to new developments.” *Id.* (quoting from the ABA Cybersecurity Handbook  
143 at p. 73).

144 “Reasonable efforts” are those which are reasonably calculated to eliminate, or at least  
145 minimize, particular, identified risks. For example, when law firm personnel work ~~if a firm~~  
146 ~~allows its staff to work~~ on client matters remotely, ~~it~~ the law firm must ensure that all data  
147 flowing to and from those remote locations and the firm’s servers or cloud storage is  
148 adequately secured. The particular method or methods selected (VPN, encryption, etc.) will  
149 reflect the firm’s due consideration of the risks, the relative ease of use of different security  
150 precautions, time that would have to be spent training staff, and the like. Some security  
151 precautions are so readily available and user-friendly (such as the ability to locate and lock  
152 down portable devices in the event of loss or theft), that failure to implement them could be  
153 deemed unreasonable. Others will require a deeper assessment.

154 Finally, in law firms with subordinate lawyers, the lawyers with management or supervisory  
155 responsibilities should be aware of their obligations under rules 5.1 and 5.3. Rule 5.1(a)  
156 requires lawyers with “managerial authority in a law firm [to] make reasonable efforts to  
157 ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the  
158 firm comply with these rules and the State Bar Act.” Thus, lawyers with managerial authority  
159 within a law firm must make a reasonable effort to establish internal policies and procedures  
160 designed to protect confidential client information from the risk of inadvertent disclosure and  
161 data breaches as the result of technology use, which includes monitoring the use of technology  
162 and office resources connected to the internet and external data sources. ABA Formal Opn. No.  
163 18-483. The law firm should also consider whether they are required to proactively establish~~ing~~  
164 protocols for responding to and addressing potential data breaches. Rule 5.1(b) requires  
165 supervisory attorneys to ensure that subordinate attorneys within the firm comply with the  
166 rules and policies and procedures established by the firm. And rule 5.3 makes these principles  
167 applicable to non-lawyer staff.

168 Thus, part of the risk assessment process should include reasonable efforts to ensure that all  
169 firm members appreciate the risks involved in keeping confidential client information on  
170 electronic systems and the steps that the firm’s managers have implemented to minimize the  
171 risk of unauthorized disclosure. Because the risk-assessment process is on-going, particularly  
172 with the introduction of new technologies and new threats, this duty would require managers  
173 and supervisors to establish ongoing and evolving protective measures with respect to the use  
174 of its technology, and regularly monitoring the same, and to keep subordinate lawyers and staff  
175 up to date as new measures are implemented.

176 However, rule 5.2 makes clear that subordinate lawyers have independent ethical obligations to  
177 protect confidential client information as part of their duty of competence. Thus, subordinate  
178 lawyers should not blindly follow firm technological rules that are clearly antiquated or fail  
179 comply with their ethical obligations when no rules are established by law firms but should be.

180 **Duty of Disclosure**

181 Rule 1.4(a)(3) and Business and Professions Code section 6068(m) require attorneys to keep  
182 their clients<sup>4</sup> “reasonably informed about significant developments” relating to the attorney’s  
183 representation of the client. Neither rule nor case law ~~clearly~~ define what events qualify as  
184 “significant.” (See, e.g., Tuft et al., *Cal. Practice Guide: Professional Responsibility* (The Rutter  
185 Group 2018) § 6:128, acknowledging that what is “significant” under these provisions varies  
186 with each client’s needs and the nature of the representation.) Nevertheless, the relevant  
187 authorities have uniformly concluded that the misappropriation, destruction, or compromising  
188 of ~~client~~ confidential client information, or a cyber breach that has significantly impaired the  
189 lawyer’s ability to provide legal services to clients, is a “significant development” that must be  
190 communicated to the client. See, e.g., ABA Formal Opn. No. 18-483 at 10; New York State Bar  
191 Association Ethics Opn. No. 842 (2010) (involving a data breach of a cloud storage provider);  
192 ABA Formal Opn. No. 95-398.

193 ABA Formal Opn. No. 18-483 describes a “data breach” as a “data event where material client  
194 confidential information is misappropriated, destroyed, or otherwise compromised, or where a  
195 lawyer’s ability to perform the legal services for which the lawyer is hired is significantly  
196 impaired by the episode.” ABA 18-483 at p. 4.<sup>5</sup> Thus, not all events involving lost or stolen  
197 devices, or unauthorized access to technology, would necessarily be considered a data breach.  
198 Consistent with their obligation to investigate a potential data breach, however, lawyers and  
199 law firms should undertake reasonable efforts, likely through the use of individuals with  
200 expertise in such investigations, to ascertain, among other things, the identity of the clients  
201 affected, the amount and sensitivity of the client information involved, and the likelihood that  
202 the information has been or will be misused to the client’s disadvantage. This will assist in  
203 determining whether there is a duty to disclose. If the lawyer or law firm is unable to make such  
204 a determination, the client should be advised on that fact. *Id.* at p. 14.

205 Lawyers and clients may also differ as to what events would trigger the duty to disclose. The  
206 key principle, however, in considering whether the event rises to the level of a data breach, is  
207 whether the client’s interests have a “reasonable possibility of being negatively impacted.”  
208 ABA 18-483 at 11. Certainly disclosure is required in situations where a client will have to make  
209 decisions relevant to the breach, such as the need to take mitigating steps to prevent or  
210 minimize the harm, or to analyze how the client’s matter should be handled going forward in  
211 light of a breach. When in doubt, lawyers should assume that their clients would want to know,  
212 and should err on the side of disclosure.

213 **If Disclosure to Clients is Required, When and What Must be Disclosed?**

---

<sup>4</sup> This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. See discussion of this in ABA 18-483 at p. 13-14.

<sup>5</sup> The Committee believes this description is useful in understanding what constitutes a data breach for the purpose of this opinion and discussion, and has adopted the same approach here.

214 In all cases involving a data breach, disclosure to clients must be made as soon as reasonably  
215 possible so the affected clients can take steps to ameliorate the harm.<sup>6</sup> For example, affected  
216 clients might want or need to change passwords and modify or delete on-line accounts.  
217 However, it is certainly reasonable for the lawyer, through the use of a security expert, to  
218 attempt ascertain the nature and extent of the potential breach prior to communicating this  
219 information to the client. The more that is known related to the breach, including exactly what  
220 information might have been accessed, the better the response plan. Given the obligation to  
221 preserve client confidences, secrets and propriety information, it is appropriate to assume that  
222 reasonable clients would want to be notified if any of that information was acquired or  
223 reasonably suspected of being acquired by unauthorized persons.

224 With respect to the details of a required disclosure, the attorney “shall explain a matter to the  
225 extent reasonably necessary to permit the client to make informed decisions” as to what to do  
226 next, if anything. (Rule 1.4(b)). “In a data breach scenario, the minimum disclosure required to  
227 all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of  
228 its information, or that unauthorized access or disclosure is reasonably suspected of having  
229 occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which  
230 client information was accessed or disclosed.” ABA 18-483 at p. 14.

231 Lawyers may also have notification obligations under Civil Code section 1798.82 and federal  
232 and international laws and regulations such as HIPAA and the EU General Data Protection  
233 Regulation.

### 234 **The Factual Scenarios**

235 Although Attorney A’s laptop is stolen and it could be used to access confidential client  
236 information, the risk of unauthorized access to such information was mitigated by Attorney A  
237 and law firm’s policies for addressing these types of cyber risks. First, Attorney A did not store  
238 confidential client information on the laptop, but only used the laptop to access such  
239 information remotely. Second, Attorney A had a biometric password on the laptop reducing the  
240 chances that it could be hacked by an unauthorized user. Third, Attorney A’s law firm had the  
241 ability to quickly and easily locate, lock and wipe clean the laptop, almost guaranteeing that  
242 there was no unauthorized access to any confidential client information. Under these facts,  
243 where there is no evidence of unauthorized access or harm, Attorney A would not have a duty  
244 to disclose to any client the fact that Attorney lost the laptop.

245 Attorney B’s temporary loss of a smartphone, under these circumstances, is unlikely to be  
246 considered a data breach, particularly if Attorney B can obtain assurances from the restaurant  
247 owner/staff that only the restaurant had access to it and that no one accessed the phone’s

---

<sup>6</sup> Lawyers and law firms should also consider notifying insurance carriers as soon as possible of any circumstances giving rise to a potential breach to put the carrier on notice. [While typically such acts are only covered by specific Cyber Coverage policies, not general LPL or CGL policies, these policies typically have fairly short time limits within which notice must be given.](#)

248 contents after Attorney B left. [Attorney B could have also considered](#) Because it does not  
249 appear that the data on Attorney B’s phone was misappropriated, destroyed or compromised,  
250 the temporary loss of the phone is unlikely to constitute a significant development and no duty  
251 to disclose would likely be triggered.

252 Under these circumstances, however, Attorney B and law firm should consider whether it  
253 should require all law firm attorneys to have stronger passwords, or ones that use biometric  
254 data, on firm issued smart phones or if law firm should allow their attorneys to access client  
255 data, including emails, on the attorney’s personal smartphones. The firm should also consider  
256 requiring all smart phones used for firm matters to have software installed to locate, lock and  
257 wipe devices if they are lost or stolen, [and specific protocols for managing such scenarios.](#) Next  
258 time, Attorney B may not be so confident in Attorney’s assessment that no client data was  
259 accessed, particularly if the phone is one day stolen. [For example, it is possible that Attorney B’s  
260 cell phone provider could have locked down the phone remotely, but Attorney B did not  
261 consider this option or look to the law firm for advice on handling this situation.](#) Finally, when  
262 electronic devices are temporarily lost or misplaced, the law firm should consider whether its  
263 policies should include requiring its IT team to examine those devices once the device is  
264 recovered to determine whether any unauthorized access took place.

265 The situation of Law Firm C involves a common entry point for hackers: malware attached to a  
266 seemingly legitimate e-mail, also referred to as “phishing.” Given the ubiquity of this method of  
267 gaining access, solo practitioners and firms must consider implementing reasonable  
268 precautions, such as staff and attorney training warning of this risk and protocols for handling  
269 in-coming e-mails. Law Firm C has certainly been inconvenienced by the cyber breach, but the  
270 firm has confirmed that none of its clients were actually or potentially harmed because no  
271 confidential [client](#) information was accessed, and the short delay did not impair the firm’s  
272 attorneys from continuing to provide necessary legal services to its clients. Therefore, the firm  
273 would not be required to disclose the incident. On the other hand, if the consultant could not  
274 preclude actual or potential unauthorized access, a risk of client harm remains and disclosure  
275 would be required.

276 Attorneys who keep confidential information on their ~~portable~~ devices ought to be aware that  
277 accessing public Wi-Fi or other unsecure networks may open another access point for hackers.  
278 This is illustrated by Attorney D’s exposing confidential information to anyone with the  
279 capability of electronically “eavesdropping” on the Attorney’s keystrokes. Attorneys who work  
280 on client matters remotely must consider the risks of harm and take reasonable precautions, as  
281 discussed above, to prevent unauthorized disclosure. Cal. State Bar Formal Opn. No. 2010-179  
282 at p. 6 (discussing use of laptop in unsecured and secured settings). Attorney D’s failure to  
283 secure their on-line communications exposed confidential information to a hacker and it is  
284 unknown if, or to what extent, the hacker would or could use such information.

285 Since the law firm was able to confirm the unauthorized access of confidential client  
286 information, Attorney D and law firm must notify the client Company as soon as possible.  
287 Although it is unknown if or how the hacker might use the information, because of the sensitive

288 nature of the information to Company’s business, the misappropriation would constitute a  
289 significant development and require appropriate notice to the client. “[D]isclosure will be  
290 required if material client information was actually or reasonably suspected to have been  
291 accessed, disclosed or lost in a breach.” ABA 18-483 at p. 14.

292 Once a disclosure is made, Attorney D and law firm can evaluate with Company the likelihood  
293 that the information will be used by the hacker and may decide to speed up the timeline for  
294 obtaining the relevant patents related to the information that was inadvertently disclosed to  
295 mitigate potential harm<sup>7</sup>. Of course, the event would also require Attorney D and law firm to  
296 take appropriate remedial steps in terms of evaluating the firm’s policies related to attorney’s  
297 accessing firm devices from unsecured locations. It should also consider reinforcing policies  
298 requiring attorneys to promptly address any irregularities or suspicions related to potential data  
299 breaches with the firm’s technology officers as soon as they are discovered.

### 300 CONCLUSION

301 The use of computers and portable electronic devices by lawyers is now ubiquitous and has  
302 increased the risk of client confidential [client](#) information being accessed by unauthorized  
303 users. Lawyers must assess the risks involved in the use of electronic devices and systems that  
304 contain, or access, confidential client information and to take reasonable precautions to ensure  
305 that that information remains secure. This duty extends to law firms whose managers must  
306 make a reasonable effort to establish internal policies and procedures designed to protect  
307 confidential client information from the risk of inadvertent disclosure and data breaches as a  
308 result of technology use, to monitor such use, and to stay abreast of current trends and risks.  
309 The creation of a data breach response plan ~~is also recommended~~ [may also be required](#) to  
310 identify the risks posed to the firm’s then-current use of technology and feasible precautions.

311 This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of  
312 the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of  
313 California, its Board of Trustees, any persons, or tribunals charged with regulatory  
314 responsibilities, or any licensee of the State Bar.

---

<sup>7</sup> [In addition, because Attorney D’s handling of confidential client information may constitute an error giving rise to a potential malpractice claim, Attorney D and law firm should also consider whether a conflict of interest has arisen between the law firm and client such that the law firm should also comply with rule 1.7 in disclosing this significant development to client. \(See also Cal. State Bar Formal Opn. No. 2019-19\)](#)