Working Group #3 Confidentiality Self-Assessment Form

Colo. RPC 1.6 addresses the confidentiality of client information and when disclosure is prohibited or permitted. Confidentiality applies not only to matters communicated in confidence by the client, but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules. [Cmt. 3 to Rule 1.6]. Confidentiality survives the conclusion of the attorney-client relationship.

Many issues regarding disclosure of confidential information are preventable; thus, written policies to educate lawyers and staff, and review of such policies through the following form, will aid in preventing such disclosures. Some disclosures, however, are inadvertent; for those situations, the lawyer should be aware of how such disclosures can happen, and operate carefully to avoid such disclosures. Technology presents additional issues, which are not always as obvious, and therefore, while preventable, must first be identified as a potential area of concern. Issues related to technology, in particular, may require additional expertise that necessitates the use of resources outside of the firm.

Questionnaire	Yes	No	N/A	Common Ethical Issues Involving Confidentiality	Other Resources
Confidentiality Policy for Employees				• Misunderstanding the breadth of Colo. RPC 1.6 • Disclosing confidential information in motion to withdraw (see also Colo. RPC 1.16) • Inadvertent disclosure such as including the wrong parties in a confidential client email, or hitting "reply" instead of "forward" when emailing (see also Colo. RPC 4.4) • Utilizing social media to discuss work, including client matters • Discussing "hypotheticals" with another lawyer where confidential information is provided (see Colo. RPC 1.6, cmt. 4) • Posting responses to online reviews of the lawyer's services • Inadvertently providing other client files or client information when returning client files • Improperly disposing of or storing client information that makes it accessible to the public	(note: we envision this section will include links to Ethics Opinions, websites, written materials, short videos)
• Does the practitioner/firm have written policies for lawyers and support staff explaining the applicable duties to preserve client confidences? If not, it is recommended the practitioner/firm develop written policies that include at minimum the following criteria discussed below.					
• If so, are such policies presented at new employee orientation and signed by the new employee?					
• If so, do such policies address when to obtain client consent for disclosure?					
• If so, do such policies specify the client's consent to disclosure should be authorized in a writing signed by the client?					

• If so, do such policies address office structure, such as public access to and visibility of client files, computer monitors, copy/fax machines, files and file storage?					
• If so, do such policies address where confidential discussions within the office may occur?					
• If so, do such policies address the security of the law office, such as who has keys to the office, who is responsible for locking the office at night, and who has off-hours access?					
• If so, do such policies address file storage onsite? • If so, do such policies address file storage offsite?					
• If so, do such policies address file disposal, such as using secure recycle or destruction of confidential materials?					
Inadvertent Disclosure					
• Does the practitioner/firm have a policy regarding what actions to take following notification of an inadvertent disclosure?					CBA Ethics Op. 108 Inadvertent Disclosure of Privileged or Confidential Documents ABA Ethics Op. 06-440 Unsolicited Receipt of Privileged or Confidential Materials See also Colo. RPC 4.4
• If so, does the practitioner/firm have a policy to notify and explain such disclosure to the client?					

Outside Vendors					
• Does the practitioner/firm have a confidentiality policy for vendors, such as cleaning staff, contract staff and computer maintenance vendors?					
• If so, is such policy in writing and signed by all vendors who access the office?					
Office Share					
• If the practitioner/firm shares space with another practitioner/firm, are there policies in place to segregate files and other confidential client information?					
Technology and Security					CBA Ethics Op. 119 Disclosure, Review and Use of Meta Data ABA Ethics Op. 11-459 Duty to Protect the Confidentiality of E-mail Communications with One's Client ABA Ethics Op. 06-442 Review and Use of Metadata
• Does the practitioner/firm have the time and expertise to oversee technology, including security?					
• Within a firm, is there a designated technology compliance officer?					
• If the above answers are "no," the practitioner/firm should consider hiring someone to assist with these tasks.					
Network/Hardware Security					
• Does the practitioner/firm have adequate physical security protection for the computer hardware used in the operation of the network?					
• Does the practitioner/firm enforce the software update process, including updating patches and antivirus software?					
• Does the practitioner/firm utilize a wireless computer network?					
• Does the practitioner/firm utilize "open" or "wi-fi" or other computer networks not controlled by the practitioner/firm?					

• If so, are adequate steps taken to protect the confidentiality of client information transmitted through or accessible by the use of those networks?					
• Does the practitioner/firm utilize publicly accessible AC power outlets?					
• If so, are adequate steps taken to protect the confidentiality of client information that may be accessible by the use of the public power outlets?					
Other Technology Used by the Firm					
• Does the practitioner/firm use smart phones or other portable digital devices in the practice?					
• If so, are those devices adequately configured to protect the confidentiality of information stored on or accessible through or by means of the phone or other digital device (such as USB drives, portable storage devices)?					
• If so, does the practitioner/firm use password-protection for portable devices?					
• If so, are those passwords routinely updated?					
Email					
• Does the firm use email to communicate to send confidential information?					
• If so, is the level of encryption utilized adequate to protect confidential information?					
• If not, are clients advised regarding the potential risks regarding email communication?					

Cloud Services					
• Does the firm use cloud services?					
• If so, where do the cloud servers reside? In the US, or elsewhere? If elsewhere, how might the laws of that jurisdiction impact confidentiality?					
• If so, does the contract with the cloud provider address confidentiality of the information?					
• Does the contract address whether the information will remain confidential should the contract end?					
Social Media					
• Does the firm have a social media presence?					
• Has the firm designated one person to update social media?					
• Has the firm designated a lawyer to review and approve content and updates to ensure no confidential information is posted?					
• Does the firm have written policies regarding employee use of social media? If so, do such policies address what information can be posted as it relates to the firm?					
Written Policies for Technology					
• Does the practitioner/firm have written policies regarding technology?					
• If so, are such policies reviewed with each new employee?					

• Do such policies address training to protect against inadvertent disclosure of confidential information? E.g., metadata.					
• If so, do such policies address the use of technology and keeping such technology, such as smart phones and computers, secure?					