# Keeping Client Confidences in the Digital Age

by J. Randolph Evans, Shari L. Klevens, and Lino S. Lipinsky

**Authors' Note**

Readers' comments and feedback on this series of "Whoops—Legal Malpractice Prevention" articles are welcomed and appreciated. References in the articles to "safest courses to proceed," "safest course," or "best practices" are not intended to suggest that the Colorado Rules require such actions. Often, best practices and safest courses involve more than just complying with the Rules. In practice, compliance with the Rules can and should avoid a finding of discipline in response to a grievance or a finding of liability in response to a malpractice claim. However, because most claims and grievances are meritless, effective risk management in the modern law practice involves much more. Hence, best practices and safer courses of action do more: they help prevent and more quickly defeat meritless claims and grievances.

The standard of skill, care, prudence, and diligence for Colorado attorneys includes taking adequate care to protect client confidences.[1] The Office of the Presiding Disciplinary Judge can discipline an attorney for the failure to maintain client confidences, or to ensure that the individuals whom the attorney manages or supervises maintain client confidences.[2] Furthermore, attorneys can face a malpractice claim for such failures. For example, clients whose attorneys failed to adequately protect their trade secrets can assert claims for professional negligence.

Despite the serious consequences of failing to maintain client confidences and secrets, many attorneys overlook this important obligation. What's more, the widespread use of electronically stored information has made it easy for even the most scrupulous attorneys to inadvertently disclose privileged information. This article addresses challenges today's attorneys face in maintaining client confidences and offers best practices for meeting this obligation.

## Keeping Secrets in the Internet Age

In the past, attorneys needed to take special care to ensure that their colleagues and employees understood the risk of innocent elevator talk or casual conversations in public settings. As legal malpractice suits illustrate, loose lips can sink ships—including business deals, settlements, cases, and negotiations.[3] Those risks pale in comparison to the risks that attorneys face in the world of social media and Internet search tools.

Data security is an even more complex challenge for law firms, as it is in many other industries. The American Bar Association reported that, in 2015, approximately one-quarter of all U.S. law firms with 100 or more lawyers had experienced a data breach through hacker or website attacks, break-ins, or lost or stolen computers or phones.[4] In 2015, 15% of all law firms, regardless of size, had reported an unauthorized intrusion into their computer files, up from 10% in 2012.[5]

## About the Authors

Randy Evans is an author, litigator, columnist, and expert in the areas of professional liability, insurance, commercial litigation, entertainment, ethics, and lawyer's law, and handles complex litigation throughout the world. He has authored and co-authored eight books and several newspaper columns. He co-chairs the Georgia Judicial Nominating Commission and serves on the Board of Governors of the State Bar of Georgia—randy.evans@dentons.com. Shari Klevens is a partner in the Atlanta and Washington, DC offices of Dentons US LLP. She represents lawyers and law firms in the defense of legal malpractice claims and counsels lawyers concerning allegations of malpractice, ethical violations, and breaches of duty. She is the chair of the firm's Defense and Risk Management Practice—shari.klevens@dentons.com. Lino Lipinsky is a partner in the Denver office of Dentons US LLP. He represents clients in real estate, trade secrets, professional liability, creditor's rights, employment, and contract cases. He is a member of the CBA Board of Governors, serves on the Board of the Colorado Judicial Institute, and is a former president of the Faculty of Federal Advocates—lino.lipinsky@dentons.com.

This Department is sponsored by the CBA Lawyers' Professional Liability Committee to assist attorneys in preventing legal malpractice. For information about submitting a manuscript or topic suggestion, contact Andrew McLetchie—(303) 298-8603, a_mcletchie@fsf-law.com; or Reba Nance—(303) 824-5320, reban@cobar.org.

Just a few months ago, in late March, the legal community was rocked by reports that intruders had broken into the computer networks of a number of venerable law firms, including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP.[6] Following those news stories, a plaintiff's attorney proclaimed his intention to file breach of contract and malpractice claims against law firms that had allegedly failed to take reasonable precautions to protect their clients' electronic files and, further, had purportedly not complied with state laws requiring notification of data breaches.[7] The evidence suggests that hackers have attempted to gain access to certain corporations' information through their outside law firms' networks because the lawyers' computer records include client trade secrets and confidential information, such as details of forthcoming mergers and acquisitions.[8] Hackers perceive law firms as "soft targets" because their networks are not as well protected as those of the firms' clients. Thus, the law firms' networks can provide the easiest means of accessing the clients' highly competitive information.[9]

A breach of an attorney's computer files could have catastrophic consequences for the clients whose confidential information has been compromised. These risks require attorneys and law firms to take a fresh look at their protocols, practices, and procedures for protecting sensitive client information. The starting point is to understand that "confidences and secrets" involve much more than just information protected by the attorney–client privilege or the work product doctrine. Instead, the scope of Rule 1.6 of the Colorado Rules of Professional Conduct extends to "all information relating to the representation [of the client], whatever its source."[10]

Under Rule 1.6, "[a] fundamental principle in the client–lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."[11] More important, this obligation continues after the attorney–client relationship has ended.[12] The protected data can include everything from the identity of a client to the termination of the relationship, and everything in between.

## Best Practices

In light of the lawyer's obligations under Rule 1.6, combined with the increased risk associated with social media and other technology, law firms should adopt and implement specific protocols, practices, and procedures to effectively maintain client confidences and secrets in the Internet age. To be clear, the applicable rules already mandate that attorneys maintain client confidences and secrets. Furthermore, because attorneys are charged with ensuring that others employed by the law firm maintain client confidences and secrets, the protocols also ensure that employees who are not members of the bar, as well as those who are, understand the obligation.[13] Given how much the use of electronically stored information has changed the practice of law over the last two decades, attorneys must take the steps necessary to protect their client confidences and secrets in electronic, as well as in hard copy, form.

There is no substitute for adopting and communicating to employees the steps needed to maintain confidences and secrets. Effective protocols, practices, and procedures should be in writing and should be communicated regularly to every employee of the practice.

Attorneys must maintain sensitive client information in three principal areas: (1) hard copy documents, (2) oral communications, and (3) electronically stored information. Each area presents its own challenges, and the steps for preserving confidences and secrets will vary depending on the size and nature of the law office. The best practices for protecting client confidences in each area are discussed below.

### *Hard Copy Documents*

Hard copy documents generated during the course of a representation often contain sensitive client information. All law practices should adopt a protocol for addressing the various categories of hard copy documents, including financial documents (such as billing records), documents generated during the course of the representation, and other related documents that may not be client-specific.

In addressing these categories, the attorney should consider document maintenance, retention, and destruction protocols. For document maintenance, the attorney should take reasonable steps to ensure that confidential files are stored in secured areas that are not publicly accessible. In practical terms, this means files should not be stored in conference rooms, lobby areas, hallways used by non-employees, or other locations that are not segregated and secure.

Document retention policies should be communicated in writing to the client at the outset of the attorney–client relationship, and should address the method, duration, and place of retention. The best practice is to include the document retention rules in the engagement letter or the fee agreement. These rules should contain any policies regarding originals, the client's right to the documents, and the notification procedures the attorney will follow regarding the ultimate disposition of the documents following the conclusion of the engagement.

Document destruction policies also should be communicated in writing. The most important component of such a policy is uniformity. Document destruction should not vary according to indefinite rules applied on an ad hoc basis or at the discretion of an attorney or law firm employee. Inconsistent rules invite heightened scrutiny when a destroyed file involves a matter in dispute. The safer course is to adopt and implement uniform rules regarding the length of time documents will be maintained, and the notifications provided to clients before a document is destroyed.

### *Oral Communications*

Communications that take place outside of the law office and concern client matters should be discouraged, unless they occur in the course of providing legal services. Clients consider their matters confidential and attorneys should strive to ensure they stay that way.

Effective risk management includes training law firm personnel on the importance of maintaining client confidences and secrets, and the potential consequences of failing to do so. Examples of situations in which the issue may arise, such as inquiries from outside the office, are helpful in defining the boundaries and explaining how to handle various situations. For example, many law firms use in-house public relations or media consultants to address media inquiries regarding the firm's representations. Funneling media inquiries through a centralized source within the firm helps ensure that an attorney does not disclose confidential information to a reporter. Simply trusting employees to know the boundaries is too risky.

Leading by example is important. Attorneys who routinely discuss confidential matters with others without regard for secrecy should not be surprised when others in the law firm do the same. The best strategy is to adopt a strict confidentiality standard and then follow it.

### *Electronically Stored Information*

In today's high-tech world, there is no substitute for adequate security protocols prepared by professionals. Whether the attorney is a solo practitioner or works for a large law firm, clients expect adequate security protocols to protect their information. This means that computer systems and Internet access need to be secure; non-secure access for ease of use is no longer an option. Accordingly, law firms must take the necessary steps and incur the expenses required to ensure that adequate security protocols are in place to protect client information. Although there are minimum standards of protection, each firm should review the following procedures to determine which best fit the needs of its clients and practice:

- conducting frequent training for all lawyers and staff regarding the firm's protocols, policies, and procedures for protecting client data;
- teaching lawyers and staff online common sense, including identification of "phishing" and other potentially dangerous emails, as well as the risk of clicking on links contained in suspicious emails;
- consistently using robust passwords that include both numbers and characters other than letters or numbers;
- requiring frequent password changes;
- using encryption technologies to protect hardware and other storage media;
- timely updating antivirus software;
- employing reputable firewalls;
- restricting the copying of client data onto flash drives, phones, and similar portable devices that can easily be misplaced or stolen;
- prohibiting use of personal devices for law firm data and communications;
- adopting policies requiring immediate reporting of any data breaches, system intrusions, or loss of devices containing client data;
- ensuring that all third-party vendors have adopted and follow state-of-the-art security protocols;
- barring attorneys and staff from using email services that mine user data (e.g., Gmail) for work-related communications;[14]
- deleting personal information, such as Social Security numbers, from electronically stored records;
- developing and testing incident response and data recovery plans;
- adopting and implementing retention and deletion policies clearly stating that client data is to be stored no longer than necessary; and

- engaging a data security consultant for a thorough security audit if the firm does not have its own IT staff.

Although the above steps are not necessarily required, they are best practices for security within the law office that can go a long way toward protecting client confidences and secrets.

## Conclusion

Attorneys must remain vigilant so that their clients' confidences and secrets do not fall into the wrong hands. The ubiquity of electronically stored information has created new challenges for protecting nonpublic client information from inadvertent disclosure or data theft. Attorneys should consider adopting some or all of the best practices discussed in this article to satisfy their duty to preserve client confidences and secrets.

### Notes

1. Colo. RPC 1.6, cmt. [2]. *See also* Colo. RPC Preamble [4].
2. Colo. RPC 1.6; Colo. RPC 5.3.
3. *See, e.g.*, *People v. Underhill, Jr.*, No. 15PDJ040 (Colo. Aug. 12, 2015) (attorney suspended for disclosing confidential client information in response to client's Internet criticism). *See also People v. Albani*, 276 P.3d 64, 70 (Colo. 2011) (finding attorney violated Colo. RPC 1.6(a) when he revealed confidential client information concerning the client's decision to reject a plea offer).
4. Friedman, "ABA Survey: Data Breaches Rising at Large Firm," Big Law Business Legal Communities (Sept. 23, 2015), https://bol.bna.com/aba-survey-data-breaches-rising-at-large-firms.
5. Maleske, "1 in 4 Law Firms Are Victims of a Data Breach," Law360 (Sept. 22, 2015), www.law360.com/articles/705657/1-in-4-law-firms-are-victims-of-a-data-breach.
6. Hong and Sidel, "Hackers Breach Law Firms, Including Cravath and Weil Gotshal," *Wall Street J.* (Mar. 29, 2016), www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.
7. Coe, "BigLaw in Crosshairs as Firm Plans Data Breach Litigation," Law360 (Mar. 31, 2016), www.law360.com/bankruptcy/articles/778540?nl_pk=a538023a-55b2-4181-afdb-0d9643ae9d32&utm_source=newsletter&utm_medium=email&utm_campaign=bankruptcy; CRS § 6-1-716(2) requires Colorado businesses to notify the affected individuals in the event such individuals' "personal information" stored on the business's computer system is compromised through a security breach.
8. Hong and Sidel, *supra* note 6.
9. Meleske, "A Soft Target for Hacks, Law Firms Must Step Up Data Security," Law 360 (Sept. 23, 2015), www.law360.com/articles/706312/a-soft-target-for-hacks-law-firms-must-step-up-data-security.
10. Colo. RPC 1.6, cmt [3].
11. Colo. RPC 1.6, cmt [2].
12. Colo. RPC 1.9(c)(2); Colo. RPC 1.9, cmt. [1].
13. *See* Colo. RPC 5.3.
14. Hundreds of companies collect data generated from online activity, primarily to gain insight into consumer preferences. *See* Morris and Lavandera, "Why Big Companies Buy, Sell Your Data," CNN.com (Aug. 23, 2012), www.cnn.com/2012/08/23/tech/web/big-data-acxiom. Furthermore, one commentator has suggested that attorneys should avoid using Gmail for privileged communications because Google scans emails and engages in data mining. *See* Neil, "Does Using Gmail Put Attorney-Client Privilege at Risk?" ABAJournal.com (Oct. 8, 2014), www.abajournal.com/news/article/does_using_gmail_put_attorney_client_privilege_at_risk. ■