fucile & reising | LLP

September 2019 WSBA *NWLawyer Ethics & the Law* Column

Electronic Files: Same Duties, New Dynamics

By Mark J. Fucile
Fucile & Reising LLP

One of the most significant changes in law practice over the past decade has been the transformation of law firm files from paper to cloud-based electronic form. Although our core duties of competence and confidentiality in managing our files have not changed, the electronic form has altered the dynamics of those duties significantly. Not so long ago, for example, "file security" meant making sure the last person leaving the office in the evening locked the door. Today, by contrast, "file security" involves protecting electronic information from threats that were largely unknown to law practice a generation ago. That doesn't mean that physical security is unimportant—quite the contrary in an era when the "file room" is often literally carried around on every firm laptop. The convenience and efficiency of electronic files, however, have also brought new challenges in protecting them.

In this column, we'll first survey the basic principles that govern our use of cloud-based electronic files. We'll then examine how they apply in the context of storage, retrieval and preservation of electronic files.

Basic Principles

The title to Comments 18 and 19 to RPC 1.6 neatly summarize our basic duties of file management: "Acting Competently to Preserve Confidentiality."

The twin comments underscore that protecting client confidentiality is a central element of competently representing our clients. RPC 1.6(c), for example, which is patterned on its ABA Model Rule counterpart and was added to the Washington RPCs in 2016, states: "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." Comment 18, which was amended at the same time, elaborates on this duty, ties it directly to competence and includes supervision of third-party vendors enlisted in providing our legal services: "Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."

These duties are not simply regulatory requirements that may subject a lawyer to regulatory discipline. "Competence" in a regulatory sense echoes the "standard of care" in the legal malpractice context—with WPI 107.04 noting: "An attorney has a duty to use that degree of skill, care, diligence, and knowledge possessed and used by a reasonable, careful, and prudent attorney in the State of Washington acting in the same or similar circumstances." Comment d to

Section 60 of the *Restatement (Third) of the Law Governing Lawyers* (2000) casts the duty of confidentiality, in turn, in fiduciary terms: "This [duty] requires that client confidential information be acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality."

State data breach notification laws, such as RCW 19.255.010, add two further dimensions to electronic file management. First, they essentially codify a law firm's duty to take reasonable measures to secure personal information such as Social Security and credit card numbers. Second, if there is a breach, they require notification to both clients and non-clients whose information has potentially been exposed. The Washington Attorney General's Office has a variety of resources for businesses on its web site focusing on Washington's data breach notification laws—along with a series of sobering annual reports that starkly illustrate the extent of the risk in Washington. Law firms should also carefully review their malpractice insurance policies to make sure they include data breach coverage.

Storage

WSBA Advisory Opinion 2215 (2012), which is available on the WSBA web site, addresses two key facets of cloud-based file storage: selection of a vendor; and the continuing duty to evaluate the service chosen.

On the former, Advisory Opinion 2215 notes that no one set of static guidelines is—or will remain—appropriate in light of ever-changing technology. Instead, Advisory Opinion 2215 offers a flexible set of considerations in evaluating vendors:

> "1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
>
> "2. Evaluation of the provider's practices, reputation and history.
>
> "3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
>
> "4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
>
> "5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer's stored data.
>
> "6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.

> "7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider."[1]

On the latter, Advisory Opinion 2215 emphasizes that because both technology and threats are constantly evolving, lawyers and their firms must also continually evaluate the suitability of the system being used:

> "Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider. Over time, a particular provider's security may become obsolete or become substandard to systems developed by other providers."

In 2018, the ABA issued a comprehensive opinion—No. 483, which is available on the ABA web site—that echoes this advice in the specific context of monitoring for cyberbreaches.

With both initial selection of a vendor and continued evaluation of the system used, we do not have to become computer programmers. But, if we don't have sufficient technical competence in-house, we need to get that assistance through, for example, an independent technology consultant. Comment 8 to RPC 1.1 on competence requires lawyers to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant

technology[.]" In other words, if we are going to use a particular technology like cloud-based file storage, we can't "plead ignorance."

Retrieval

When files were solely in paper form, "retrieving" a file typically meant walking to a storage location within a lawyer's office ranging from a "file cabinet" to a "file room." Cloud-based electronic files, by contrast, put a security accent on file retrieval and use as well.

Although some elements of retrieval are the responsibility of the storage vendor, lawyers themselves play a vital role in three key aspects of file security.

First, lawyers are on the front line in terms of how they connect electronically to their cloud-based files. Often, this will occur within the security perimeter of a protected office network. The very mobility of cloud-based files, however, enables to lawyers to work far from traditional "brick and mortar" offices ranging from "co-working" spaces to airport lounges.[2] Regardless of the location, the lawyer accessing cloud-based files must take reasonable precautions—consistent with RPC 1.6(c) noted earlier—to ensure that the connection is secure.[3] Depending on the circumstances, this may mean, for example, using a "virtual private network" if connecting to the internet through a wi-fi network or using an encrypted cell system connection.

Second, again reflecting the very mobility of electronic files, lawyers working outside their offices need to take care that confidential client information cannot readily be seen by others. An IP lawyer working on a commercially sensitive matter for a high-tech client, for example, likely would not want to review key proprietary documents on a large laptop screen in the middle seat of a crowded airplane. Comment 18 to RPC 1.6 emphasizes that the particular security measures implemented will vary with the situations encountered—in other words, one size does not fit all.

Finally, in addition to electronic security, lawyers need to remain mindful of physical security. As noted earlier, today a lost mobile device may be the functional equivalent of losing an entire law firm "file room." Therefore, lawyers need to understand and use basic security features commonly built into most mobile devices today such as password protection, hard-drive encryption and remote "kill switches" that can be activated if a device is lost or stolen.

Preservation

Both the attorney-client privilege (*see Martin v. Shaen*, 22 Wn.2d 505, 511, 156 P.2d 681 (1945)) and lawyer confidentiality obligations (*see* RPC 1.9(c)) generally apply to closed files. Therefore, the file management duties discussed

earlier do not end when we have completed work but retain the file involved.[4]

Electronic files present their own unique challenges in this regard.

With the shift to electronic-only files, questions can occasionally arise when a former client requests a paper copy instead. WSBA Advisory Opinion 2023 (2003) has long counseled that, once original documents with independent legal significance in their paper form such as an original will are returned to a client, a lawyer is free to convert the file into electronic form for storage. A recent ABA opinion on file transition—Formal Opinion 471 (2015)—notes that generally a client is entitled to a form that will protect the client's interest. A new Oregon opinion on file management—Formal Opinion 2017-192 (2017)—picks up this thread and concludes that an electronic copy will typically suffice given the prevalence of computers today and that a firm could ordinarily charge for what amounts to a second copy if requested in paper form by a former client. The Oregon opinion cautions, however, that "[i]n some limited situations, such as when an in-custody client may not have regular computer access, a lawyer may be required to provide a file maintained in an electronic-only format in a format that can be accessed or read by the client."[5] The principal Washington opinion on file transition generally, Advisory Opinion 181 (rev 2009), has long noted that lawyers and clients can agree contractually on file disposition issues in an

engagement agreement. A conservative approach to electronic-only files, therefore, would be to include a specific provision requiring the client to bear the cost of producing an additional paper copy.

Although the RPCs generally do not impose any particular file retention period,[6] both the WSBA and most malpractice carriers have file retention guidelines that reflect the kinds of legal work involved and the practical limits on a former client asserting a claim. The WSBA recommendations are available on its web site. Cloud-based file repositories are typically both more convenient and generally less expensive than their paper counterparts. At the same time, "preservation" in electronic form also implies a continued ability to access the information involved. Firms should consider, for example, the electronic format used and whether information stored in that format will still be readily accessible for the duration of any recommended preservation period.

Similarly, firms should also assess how files can be securely erased on both cloud-based systems and physical devices when the recommended preservation period has come and gone. In particular, portable devices that "mirror" cloud-based files should have their storage systems securely destroyed by a reputable recycler when they have reached the end of their useful lives.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, regulatory and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is also a former member of the Oregon State Bar Legal Ethics Committee and is a current member of the Idaho State Bar Section on Professionalism & Ethics. Mark writes the Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the Ethics & the Law column for the WSBA *NWLawyer* and is a regular contributor on legal ethics to the WSBA *NWSidebar* blog. Mark is a contributing author/editor for the current editions of the OSB Ethical Oregon Lawyer, the WSBA *Legal Ethics Deskbook* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches legal ethics as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.

---

[1] ABA Formal Opinion 08-451 (2008) addresses supervisory duties generally under ABA Model Rule 5.3 in the context of out-sourced services. Washington RPC 5.3 is patterned on its ABA Model Rule counterpart.

[2] WSBA Advisory Opinion 201601 (2016) discusses electronic mobility issues in the specific context of "virtual" offices but its advice applies with equal measure to lawyers generally who practice outside their traditional offices.

[3] *See also* ABA Formal Opinions 477R (2017) and 99-413 (1999) that address related issues of securing confidential attorney-client communications in the electronic environment.

[4] Client original documents that have independent legal significance in paper form should be returned to the client at the completion of a matter under RPC 1.16(d).

[5] OSB Formal Op. 2017-192, *supra*, at 4.

[6] RPC 1.15A(c)(3) generally requires trust account records to be maintained for seven years.