Chicago Daily Law Bulletin®

Volume 164, No. 134 Serving Chicago's legal community for 163 years

Cloud helps empty filing cabinets but know the ethical side of it

It's all too common to find law firms busting at the seams with an avalanche of paper. Some might say it's in our nature. The importance of "the original" of a document begins in the hallowed halls of law school.

Paper can be trusted, even revered. What better way to authenticate something but to hold it in your hands while examining it, before preserving it into a categorized and alphabetized filing system.

That just makes sense. Or, at least it did.

Digital information can be created, altered, copied, stored and shared far faster and cheaper than paper. As laws, rules and processes change to allow for better and more secure data storage and transmission, law firms join other industries working to reduce their paper and physical storage use and costs by "going to the cloud" with their data.

Lawyers have an extra hurdle to jump with the ethical obligations to their clients' data.

Not only must they ensure the security of their clients' confidential information, in storage and transmission, they also have an ethical obligation to the ongoing control of the "client file." The client has a vested right to the surrendering of the client's documents or a copy of them. See "Maintenance of Client Files and Records," ISBA Opinion 17-02; "Former Client Access to Lawyer's File," ISBA Opinion 01-01.

Not paperless, but less paper

Lawyers may use cloud-based data storage of confidential information while still protecting their client confidentiality responsibilities. More than 20 state bar associations have issued ethics opinions on this topic and all have reached the conclusion that lawyers may ethically use cloud computing, so long as they exercise reasonable care to keep client information and files confidential.

Some of those opinions may be found on the American Bar Association's Legal Technology Resource Center's page (note that it is an incomplete list with Illinois and possibly others omitted).

Much of the data you are already utilizing and communicating with your clients are already being stored and managed out of cloud-based technology.

Your practice management software may be entirely managed and hosted in the cloud. When you cannot e-mail certain documents due to their size, you might already be turning to services like Dropbox, Microsoft OneDrive and Google Drive for easy file storage and sharing — they're all cloud-based.

As you know by now, especially if you live in one of the 30-plus states that have adopted it, Rule 1.1 requires attorneys to keep abreast of changes in law and its relation to technology.

This means that attorneys need to be aware of the benefits and risks of technological applications and the standards that regulate them. You certainly don't have to have a degree in computer science to know how it all works, you just need to take reasonable due diligence to know it is secure.

Likewise, Rule 1.6(e) requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Such access prevention responsibilities do not end when the information isn't just sitting in a file folder on your desk.

The confidential client information transmitted via electronic means must be properly safeguarded, demanding that you employ and oversee third-party providers with the same reasonable efforts.

Due diligence

So, what are "reasonable efforts" to ensure the security of cloud-stored data? How might a firm best select a cloud-based service provider and what ongoing obligations does the lawyer have to maintain that reasonable care?

When vetting a cloud-based provider, or any technology vendor really, it is important to recognize that best practices and professional standards evolve alongside technology. Just as our technology tools evolve, so must our factors in evaluating the quality and abilities of our hardware and software providers.

If you are not familiar with current cloud-computing industry standards and safeguards, you should at least know what kinds of questions to research and ask of the specific providers. Ask the company: Which industry security standards it practices, what type of security audits will it provide, and so on.

The ISBA Professional Conduct Advisory Opinion 16-06 outlines seven nonexhaustive reasonable inquiries and practices lawyers could engage in to select a cloud-based service provider:

1. Reviewing cloud-computing standards and familiarizing oneself with the appropriate safeguards that should be employed.

2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections and encryption.

3. Investigating the provider's reputation and history.

4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches.

5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information.

6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data.

7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.

PROFESSIONALISM ON POINT

MARK C. PALMER

As professionalism counsel at the Illinois Supreme Court Commission on Professionalism, Mark C. Palmer promotes civility and delivers statewide professionalism programming, including its mentoring program, across Illinois to lawyers and law students.

Lawyers may use cloud-based data storage of confidential information while still protecting their client confidentiality responsibilities.

Ongoing duty

As the applications of cloud computing evolves, so must our security and compliance inquiries to keep our practices and our clients safe.

As Illinois Opinion 16-06 states: "Pursuant to Rules 1.6 [Confidentiality of Information] and 5.3 [Responsibilities Regarding Nonlawyer Assistance], a lawyer has ongoing obligations to protect the confidentiality of client information and data and to supervise non-lawyers. Future advances in technology may make a lawyer's current reasonable protective measures obsolete. Accordingly, a lawyer must conduct periodic reviews and regularly monitor existing practices to determine if the client information is adequately secured and protected. See, e.g., Arizona Ethics Op. 09-04 (2009); Washington State Bar Association Advisory Op. 2215 (2012)."

Along with asking questions, you need to read the provider's contract or terms and conditions, which are very likely going to be different if you are using a free service instead of a paid service.

The difference in what could happen to your clients' information if the service is canceled is an example of what could be at issue. (Think: Rule 1.16(d) requiring that upon termination, you "shall take steps to the extent reasonably practicable to protect a client's interests" including surrendering the client's file.)

Additionally, some opinions suggest you obtain the informed consent of your client before placing confidential information in the cloud. To that end, think about what language you could put in your retainer agreement to memorialize it.

Like many technology advances before it (read: computer, fax machine, e-mail), cloud-based storage has become the standard method for storing and sharing data.

The legal profession, like other industries, must make ongoing reasonable efforts in choosing and reviewing our service providers. We owe it to our clients, ethically and professionally.