The Ethics of File Sharing for Attorneys

Data protection responsibilities, challenges and best practices for attorneys in the modern age.

Legal professionals handle a wide variety of incredibly sensitive data. Clients trust attorneys with items such as tax records, intellectual property and protected health information which, if exposed, leave clients vulnerable to criminal activity.

For this reason, a multitude of federal and state privacy laws and industry guidelines regulate the storage and transfer of sensitive data and invoke severe financial or even criminal consequences for noncompliance. Many attorneys are subject to such penalties without even knowing it.

For instance, attorneys may not think they need to worry about the Health Information Portability and Accountability Act (HIPAA) if they do not practice health law. But personal injury, malpractice, family, and Social Security law often require the handling of medical records, which are protected under HIPAA. Recent updates to HIPAA regulations have enforced stricter compliance by third parties, attorneys included[1]

Real estate attorneys may be affected by the creation of the Consumer Financial Protection Bureau (CFPB),[2] which regulates consumer funds. Though CFPB rules are aimed largely at lenders, third parties like closing attorneys may also be liable.[3] Real estate attorneys who handle investment properties also deal with information regulated by the Securities and Exchange Commission (SEC) or state securities laws,[4] as do tax, financial, commercial, or other attorneys who deal with bank records.

Given the potentially disastrous results of noncompliance with these regulations, attorneys must take every precaution possible to secure their digital data. They should also keep a less threatening but more common problem in mind: loss of client trust. Even if they are not harmed by its breach, clients will feel personally violated if their information is exposed through poor business practices. Attorneys have an ethical responsibility to avoid this outcome by keeping client data private through good security measures.

However, most don't. The ABA TECHREPORT 2013 claimed that fewer than half of law firms encrypted their files. Worse, 25% had no security policy at all. The numbers got worse as the size of the firm in question decreased; only 11% of solo respondents reported having an Internet use policy.[5]

Why is that?
Because data security is complicated.

To achieve data security, law practices must rely on their own in-house staff or outside security consultants. Large firms often employ both. However, small to midsize practices likely don't have the resources to invest in outside help. Security falls to small IT departments, administrative staff, or practitioners themselves who are not well-trained technically. They may have a hard time keeping up with which regulations they need to follow, much less complying with them.

In these cases, practices can reduce their security burdens with data storage and transfer tools that already support privacy compliance.

File-sharing services have offered themselves as one of those tools in recent years, and the legal field increasingly uses their products.[6] However, many attorneys still have concerns about whether this is an ethical practice.

To determine whether file sharing is ethical, attorneys must ask themselves two questions:

- What are my ethical data security obligations?
- Can my file-sharing service fulfill them?

Formal ethical guidelines for data security

In some ways, the ethical guidelines that govern digital data security in the legal field predate the issue itself. The American Bar Association Model Rules of Professional Conduct, which were adopted in 1977,[7] state in section 1.6(c) that a lawyer must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." [8] In previous decades, maintaining physical barriers like locks or alarm systems and transferring documents outside of the office carefully were enough to fulfill privacy obligations. While those measures are still important, the clause should now be interpreted to include best data security practices.

Though attorneys are primarily governed by the ethical guidelines of their own state bars, the ABA Rules have been used as a model by most bar associations. In all states, the same ethical obligation to maintain client privacy through good data security is required.

Attorneys are also enjoined to serve their clients with "competent representation." (Model Rules, 1.1).[9] Today, competency includes reasonable data security measures.

Data security challenges

Unfortunately, maintaining good security is as difficult as it is important. New technologies crop up quickly, and each introduces new security weaknesses. To account for them, attorneys need the money and time to implement best practices and the knowledge of how to do so — all of which are limited resources.

Network security can be expensive. Creating secure private networks, hiring IT staff to maintain the hardware and software they require or talking to outside security consultants can cut into the yearly budget. Many people don't understand the importance of data security or the increasing threat to it, so boards of directors or other key stakeholders may not be willing to invest the funds necessary to plug the holes in their own systems.

Money pressures are matched by time pressures. The Digital Age has made us impatient; studies have shown that waiting even a few seconds for a page to load is unacceptable to some people using the Internet.[10] Clients expect the same immediate results and instant communication.

To serve this need, law offices often communicate and transfer files using email, the fastest method available. But email is only as secure as its source and destination networks. Attorneys often don't realize that every time they email, they are taking the recipient's network security on faith. They also may not have taken care of their own internal networks by maintaining firewalls and security patches. Mobile devices introduce further threat; attorneys may not think twice about emailing on their smartphones from places like the local coffee shop, whose network security is far from guaranteed.

Mobile devices also introduce the threat of simple human error. They are susceptible to damage, theft and loss. The Ponemon Institute, a data security think tank, has found that in the healthcare field loss of mobile devices is the No. 1 cause of security breach.[11] For modern professionals it's difficult to resist the temptation to take documents home on a laptop or work on the go from a tablet. But if those devices are stolen or go missing, data breach has occurred. It's almost impossible for even the most rigorous data security plan to fully account for this kind of error.

Security breach: a case study

In 2011, a Baltimore law firm discovered just how common human error is. A staff member of Baxter, Baker, Sidle, Conn & Jones took a portable hard drive out of the office and accidentally left it on the light rail. Though she discovered her mistake and went back for the device minutes later, it was already gone.[12]

The drive contained an unencrypted backup of all the firm's data, including the private health information of 161 patients of a physician client. Its loss put the firm at risk of punishment under regulatory laws like the Health Information Portability and Accountability Act (HIPAA), which protects personal health information. It put many people in danger of identity theft and other crimes by exposing their Social Security numbers and private records. More to the point, it also violated each attorney's ethical obligations by exposing client data.

This incident demonstrates the complexities of data security. The firm did have a security plan, which included taking the device out of the office as a physical protection against fire and flood. However, in doing so, they exposed the data to other kinds of risk. Though it was password-protected, the firm had not encrypted the drive, which is now standard best practice. They relied on a plan that didn't make room for mistakes.

File sharing as a data security tool

File-sharing services allow you to store information on remote servers and access it through the Internet. This process is often referred to as being "in the cloud" or as "cloud computing." When you use a file-sharing service to store and transfer records, you are relying on that service's security measures to keep the data safe.

If the service you've chosen maintains good security protocols, it can solve some of your challenges. File sharing is fast; users can still email documents, but in the form of a link to the document in the cloud rather than as an attachment. This way, security is maintained by the file-sharing service's encryption protocols rather than by the sender's or recipient's knowledge or implementation of best practices.

File sharing is often as or more cost-effective than implementing and maintaining complicated security features like virtual private networks or hiring outside IT consultants. It is less complicated than other older solutions to network security issues such as FTP or SFTP sites. File-sharing services often employ mobile apps that allow users to download encrypted files to their devices; even if they are on unsecured Wi-Fi networks, their files are protected. And because data lives in the cloud, not on a device, it's not accessible if the device is lost or stolen.

"Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications."

-The State Bar of California Standing Committee on Professional Responsibility and Conduct,
Formal Opinion No. 2010-179

Ethics opinions on cloud computing

A total of 19 state bar associations have found that cloud computing is ethical under certain conditions.[13] The consensus is that if attorneys take reasonable measures to assure themselves that the service in question secures data appropriately, third-party file storage and sharing is acceptable.

California's opinion provides a good example. The State Bar of California issued this blanket ethics opinion on the subject of the storage and transference of electronic data across various technologies, including file sharing.[14]

The last points depend on the first. If the technology in question is secure enough, then even very sensitive data can be stored and transmitted without legal ramifications to third parties and without negative impact on a client, and attorneys will be able to meet their urgent needs for speed in communication.

Ohio is even more specific. The Ohio State Bar Association addresses the question of storage in the cloud in the Informal Advisory Opinion 2013-03.15 It finds that "storing client data in 'the cloud' is a permutation on traditional ways of storing client data, and requires lawyers to follow the ethics rules that apply to client information in whatever form." In other words, the same ethics that apply to paper-and-folder file systems apply to the cloud.

The association lists 4 criteria under which cloud computing is acceptable: "competently selecting an appropriate vendor; preserving confidentiality and safeguarding the client's data; supervising cloud storage vendors; and communicating with the client." In order to meet the last 3 criteria, attorneys must take care with the first — here, an appropriate vendor is one that uses best data security practices.

Selecting a secure file-sharing service

As Ohio says, the first step to using file-sharing services ethically is selecting the right one. But here again, attorneys run into a scarcity of knowledge. Data security is not the core competency of most law practitioners. How do they know whether a file-sharing service secures data appropriately?

Unfortunately, "appropriate" is a moving target. As new security weaknesses are exposed, new protocols need to be put in place. Creating those protocols is the job of organizations like the National Institute for Science and Technology,16 which conducts ongoing security investigations and regularly updates its recommendations for best security practices.

In turn, keeping up with NIST and other regulatory standards is the job of other organizations that help companies implement best practices. If a file-sharing service has been certified through industry-recognized audits by national or international standards organizations, attorneys can be assured that its security measures are up to par.

When evaluating a service, attorneys should look for certifications such as:

- SSAE 16
- SOC 1, 2 and 3
- ISO 27001

Audits examine various features, including how a service encrypts its data during storage and transfer and whether its servers are physically secure. Attorneys should look for NIST-recommended security features such as:

- AES 256-bit encryption on servers
- Transport Layer Security encryption during transfer
- Multiple redundant datacenters with weather-and-emergency preparedness

A file-sharing service should also be able to take care of mobile security problems. Its apps should offer features like remote wipe, which allows users to delete files via the Internet if their device is lost or stolen, and multifactor authentication, which requires the entry of multiple kinds of security codes.

Administrative functions can offer extra security. For instance, thorough reporting features allow administrators to see who has downloaded a file, when, and in some cases from what IP address. This allows them to carefully track a document's lifecycle and identify any problems with unauthorized access quickly.

Another way to judge a service's security measures is by its adherence to federal regulations that govern the security of sensitive information. To comply with these regulations, services will often need to pass certain audits and employ a wide range of security features and protocols. Examining the regulations with which a service complies is one of the best tests of its security. If, for instance, a service is HIPAA compliant, then it meets the most stringent standards yet devised by the government.

Conclusion

Information technology is evolving at an increasingly rapid rate. It is becoming more complex, more efficient and more integrated with our daily lives. The ethical responsibilities that affect attorneys' interactions with today's technology — competent representation and client confidentiality — require attorneys to take all reasonable data security precautions. Legal firms can use all the help they can get.

Good file-sharing services can provide that help. Outsourcing data security needs can help firms save money and time and circumvent the problem of limited technological know-how. They can solve some of the network security challenges created by mobile devices and allow attorneys all the efficiency and convenience of the modern workplace while helping them maintain the same client privacy for which they've been ethically responsible for generations.

As attorneys continue to evaluate file-sharing services, they should keep in mind that data security is now its own ethical responsibility and that they have an obligation to make sure that the services they choose measure up. By thoroughly researching their service's security standards, attorneys can assure themselves that they are meeting the ethical obligations of their field and representing clients to the very best of their abilities.

Notes

[1] The U.S. Department of Health and Human Services, Office for Civil Rights. "Health Information Privacy; Frequently Asked Questions; Business Associates." Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/, accessed 04/01/2015.

[2] www.consumerfinance.gov, accessed 04/01/2015.

[3] Dodd-Frank Act, Consumer Financial Protection (CFPB), & ALTA Best Practices 2.0 Approved Attorney Handbook. p. 3-4. (2013). Retrieved from http://www.northcarolina.ctt.com/docs/A3%20-%20Dodd-Frank,%20CFPB%20%26%20ALTA%20Best%20Practices%20-%20Approved%20Attorney%20Handbook.pdf, accessed 03/01/2015.

[4] Sirkin, A. (2013). Securities Law Primer for Real Estate Professionals. SirkinLaw APC. [blog]. Retrieved from http://www.andysirkin.com/HTMLArticle.cfm?Article=171, accessed 04/01/2015.

[5] POJE, J. (n.d.). Security Snapshot: Threats and Opportunities. The American Bar Association ABA TECHREPORT 2013, 2-2. Retrieved from http://insidecybersecurity.com/iwpfile.html?file=pdf13%2Fcs12122013_aba_survey.pdf accessed 04/01/2015.

[6] Kennedy, D. Cloud Computing. The American Bar Association Tech Report; 2014. Retrieved from http://www.americanbar.org/publications/techreport/2014/cloud-computing.html, accessed 03/19/2015.

[7] The American Bar Association. Model Rules of Professional Conduct, Preface. Retrieved from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_preface.html, accessed 03/19/2015.

[8] The American Bar Association. Model Rules of Professional Conduct, Rule 1.6(c). Retrieved from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html, accessed 03/19/2015.

[9] The American Bar Association. Model Rules of Professional Conduct, Rule 1.1. Retrieved from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html, accessed 03/19/2015.

[10] Work, Sean. How Loading Time Affects Your Bottom Line. KISSmetrics. Retrieved from https://blog.kissmetrics.com/loading-time/, accessed 03/19/2015.

[11] ID Experts, (spons.) Third Annual Benchmark Study on Patient Privacy & Data Security, p. 1-2. Ponemon Institute. Dec. 6, 2012. Retrieved from https://www2.idexpertscorp.com//resources/single/third-annual-benchmark-study-on-patient-privacy-data-security/r-general, accessed 03/19/2015.

[12] Bishop, T. (2011, October 11). Midei's law firm loses patient data. The Baltimore Sun. Retrieved from http://docs.newsbank.com/s/InfoWeb/aggdocs/NewsBank/13A51D2A483E8110/0FF0DDC272369ADF?p_multi=MBDB&s_lang=en-US, accessed 03/19/2015.

[13] The American Bar Association. Cloud Ethics Opinions Around the U.S. Retrieved from http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html#OH

[14] The State Bar of California Standing Committee on Professional Responsibility and Conduct. Formal Opinion No. 2010-179. Retrieved from http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3D&tabid=837, accessed 03/19/2015.

[15] Ohio State Bar Association (2013). OSBA Informal Advisory Opinion 2013-03. Retrieved from https://www.ohiobar.org/ForPublic/LegalTools/Documents/OSBAInfAdvOp2013-03.pdf, accessed 03/19/2015.

[16] www.nist.gov, accessed 03/19/2015.

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.