# Maintaining Vital Law Firm Client Confidentiality: How Legal Tech Can Help

Clare Lintzenich August 24, 2021

According to the American Bar Association, 25% of all U.S. law firms have experienced at least one data breach. In other words: the risk to client confidentiality is at an all-time high.

Increased reliance on remote working arrangements, along with ever-evolving cyber threats, has resulted in an extra level of urgency for law firms to protect sensitive client data. Virtual work arrangements create various opportunities for breaches, while cyber attackers constantly seek to hack law firm security measures.

Additionally, law practices have been increasingly subjected to client data breaches caused by user errors and socially engineered attacks involving ransomware. They have been targeted by hackers that view the legal industry as an easy target based on the tendency of law firms to use outdated technologies and easily breached systems. When these breaches occur, sensitive client data can end up in the wrong hands. Clients are forced to deal with the ramifications of their information being used for nefarious reasons, while law firms must contend with potential lawsuits, ethical consequences, damaged reputations, and the loss of profitable business relationships.

The hesitancy of the legal community to embrace innovative technology has added to this vulnerability because most law firms lack both the necessary technology and strategies to deal with looming threats. Even those that have made some efforts often use platforms that are outdated and highly susceptible to data breaches. Threats constantly evolve with greater sophistication. Without a strategy for promoting client confidentiality, law firms leave their client data unprotected.

## The Ethics of Confidentiality

Lack of technology is no longer a valid excuse for client data breaches. Changes to the ABA Model Rules speak directly to the importance of technology.

ABA Model Rule 1.1: Competence, Comment [8] states, “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice including the benefits and risks associated with relevant technology, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.”

In addition, ABA Model Rule 1.6: Confidentiality states, “(c) 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.”

Client data breaches not only lead to financial consequences for law firms, but can also result in detrimental ethical challenges.

## Tips for Protecting Client Confidentiality

As law firms work to protect client confidentiality, they can implement strategies to guard against data breaches that originate both internally and externally. The following are some simple, but effective, steps:

### Minimize Human Error

The biggest vulnerability faced by any law firm, regardless of size, is employee error. Security experts estimate that more than one-third of business data breaches result from some form of employee negligence, error, or intentional act. These actions typically include phishing scams, loss of hardware, abuse of access privileges, or simple security mistakes. Law firms must identify and address these poor behaviors to effectively lessen opportunities for client data breaches.

An aware and proficient team makes the best weapon against client data breaches. Every member of firm personnel, from partner to receptionist, must understand and respect the vital importance of client confidentiality and protecting client data. Firms should provide mandatory training that promotes the highest levels of awareness and diligence. Without employee involvement, internal vulnerabilities and threats may not be identified, which can ultimately result in employees becoming the channels through which breaches occur.

### Encryption

Data encryption provides an effective technology tool for protecting sensitive data. Once encrypted, data becomes indecipherable should it wind up in the wrong hands due to loss or theft. The viewer must utilize the correct encryption key to unscramble the encrypted gibberish back into legible text.

Law firm encryption typically occurs in a couple of ways. Encryption in transit protects data as it is sent electronically within the firm or externally. This is commonly referred to as end-to-end encryption. Encryption at rest refers to the encryption of data that is stored on hard drives, laptops, or mobile devices.

But even with its high level of protection, many law firms fail to use encryption methods. According to some legal ethics experts, ABA Model Rule 1.6 classifies encryption failures as potential breaches of ethical duty should the data warrant special precautions. This risk seemingly requires law firms to evaluate whether each client matter necessitates encryption and take appropriate measures. Failing to do so could result in ethical violations.

### Regular System Updates

Tech providers consistently create new strategies for preventing system breaches, but these tactics only work when the systems and software are updated on a regularly scheduled basis. This includes VPN, antivirus, anti-spyware, and spam filters.

Unfortunately, far too many law firms implement new technologies and then fail to keep them fully updated. Without consistent updates, these tools may become vulnerable to ever-changing cyber threats. Outdated systems place client data at risk and may even open law firms up to liability

should a breach occur. Law firms need systems in place to ensure that necessary system updates occur.

### Scrutinizing Vendors

Third-party law firm vendors can also place client confidentiality at risk if they fail to follow strict security standards. These parties can create a weak link in the chain of client data that they are entrusted with during the course of business.

When choosing to work with a vendor, law firms need to closely evaluate the vendor's security protocols. They may also include specific security requirements within the controlling contract and ensure that the vendor's insurance policy adequately covers any breaches that may occur.

Legal tech companies routinely use cloud-based storage for their technologies. When managed correctly, these platforms offer great benefits to legal practices. But without proper security protocols in place, cloud storage becomes extremely vulnerable to cyber-attacks. Therefore, law firms need to ensure that cloud-based service providers maintain their networks with technical competence and top-notch security features.

## Document Security is the Tech Tool Every Law Firm Needs for Client Confidentiality

Law firms cannot ignore the role of document safety in the promotion of client confidentiality. With document management systems in place, firms benefit from multi-level security that limits access to reading, deleting, or editing sensitive documents both internally and externally.

These resources can also help firms quickly identify breaches by creating a detailed trail of everything related to a document's life cycle. Firms have access to specific information regarding who made changes and when. They can also review information about document transmission and downloads. These types of security checks protect client confidentiality and provide clients with the assurance that their information is being handled effectively.

The transfer of documents creates the biggest risk of breach. The transmittal of a document to the wrong recipient is a mistake that cannot be undone. If that document contains sensitive or confidential information, the law firm has created a substantial risk should the data be used against the firm or one of its clients. Email is largely considered the fastest and easiest method of sending documents to colleagues and clients, but it is also one of the biggest security risks a law firm can take. This highlights the importance of viable alternatives for sending secure client communications. With tools like client portals and secure document transmission systems, law firms are not forced to rely on risky email transmissions. The credentials of all recipients can be confirmed to ensure client confidentiality and prevent documents from ending up in the wrong hands.