CosmoLex by profitsolv

Your Guide to Keeping Client Data Secure

Learn how to streamline your firm's operations and deliver seamless client experiences.

Data breaches are on the rise, and they're costlier than ever for businesses.

More than 80% of organizations have experienced more than one data breach in their lifetime. If your client data remains unsecured, consider yourself playing the game of chance.

Modern technology has reached the point where strong security policies to protect client data are no longer optional. If you plan to run a compliant and ethical business, they're essential.

Still, many law firms are unsure where to begin when it comes to shoring up their cybersecurity and keeping client data safe. If you're wondering what your policy is, this guide is for you.

Why data security is essential for law firms

Securing your clients' data is part of your obligation to follow regulatory compliance laws set by the bar association. Your client giving you permission to transmit documents in an unsecured manner is not sufficient grounds to go against the rules and laws that govern your firm.

Using secure means to share data and files also demonstrates that you value your clients' trust and take their privacy seriously. This is critical for building solid relationships with your clients and earning their trust, an essential ingredient of a successful law firm.

Best practices for keeping client data secure

As a legal professional, you have a fiduciary duty to your clients to protect their interests and are held to strict ethical standards. Keeping client data secure is part of this commitment. The following three steps will give you a starting point for developing an air-tight security strategy that will protect your firm and the clients you represent.

Create a comprehensive data security policy

Good data security doesn't happen by accident; you need a plan. One of your first steps toward data security compliance should be drafting a comprehensive policy that governs your IT infrastructure and employee behavior.

Your policy should lay out the responsibilities of your IT team, including

implementing data encryption, the use of firewalls and antivirus software, and role-based access control for all applications. Next, create an acceptable use policy for staff that outlines constraints for accessing the corporate network and expectations for application and device usage.

Train your staff on data security risk mitigation

According to tech giant Verizon Wireless, human error causes 82% of data breaches. But human error, while never entirely avoidable, can be mitigated through sufficient training.

Security training for attorneys and legal professionals helps them understand how to avoid behaviors that might compromise client data, especially as threats evolve over time. Training topics may include how to:

- Spot, report, and avoid phishing emails
- Create strong passwords
- Use two-factor authentication

Data security training isn't a one-off task, either. It should be a consistent practice so that security becomes ingrained in the culture of your organization.

Invest in tools that prioritize security

Once you have secured your infrastructure and your network, you need to find a way to secure your files.

Instead of sending documents to your clients as email attachments, invest in a secure file-sharing and eSignature platform. These platforms will encrypt and store documents for you and allow clients to provide secure signatures using eSignature technology—that way, sensitive data is never left vulnerable to theft or attack.

Tools and strategies to support data security

Secure file-sharing should be a cornerstone of your firm's overall data security plan. In addition to ensuring regulatory compliance, using a robust, secure file-sharing and eSignature platform has many other benefits for your team and your clients.

Cloud-based software

Cloud-based software is increasingly an essential tool for law firms, no matter their size or practice areas. With cloud-based solutions at their disposal, firms can ensure their data and information is secure without compromising on accessibility or user-friendly features.

These days, cloud-based software tends to offer a higher level of security than that of traditional on-premises systems, thanks to advanced encryption technology and robust access controls.

Cloud-based software also eliminates common risks associated with traditional on-premises systems, such as hardware failures, malicious attacks,

natural disasters, or lack of specialized support. Instead, external providers take responsibility for ensuring servers remain secure and backed up at all times.

Finally, cloud-based software provides extensive data management options. Firms can easily add or remove users from the system and set varying degrees of access rights for attorneys, administrative staff, and clients, depending on the type of information they need access to. This keeps sensitive legal documents and data from being viewed by the wrong people.

Secure file-sharing and eSignature

Using a good secure file-sharing platform can help you overcome the risks associated with using email for client communication. Because email correspondence isn't encrypted, it's susceptible to interference, theft, and attacks from bad actors. That's why regulatory bodies sometimes consider firms that exchange sensitive client data by email to be non-compliant.

Secure file-sharing solutions allow you and your clients to enjoy the convenience of email without the threat of security breaches. This software securely stores documents for you and generates a link you can share with your clients. For even greater security, you can choose question-and-answer verification so that you know only the client can access the document.

If you need your client to upload files, there's a link for that, too. Clients can simply drag and drop their files in the designated spaces, and any uploaded communication will be readily available to authorized personnel without exposing sensitive information.

Client portals

Client portals are an ideal way for law firms to ensure data security. By providing clients with secure access to their data and documents via a client portal, lawyers can have peace of mind knowing that only authorized individuals can view client information.

Additionally, with cloud-based storage for legal documents, there's no need to worry about physical copies of files being misplaced or stolen. The cloud also ensures that documents are backed up regularly, meaning that all information will be safe in the event of a data breach or other incident.

Secure online payments

These days, online invoicing is the most secure and convenient option for law firms. Clients can settle their bills with a secure link, eliminating the guessing game of sending bills by mail and saving you money on overhead costs. Because clients can click and pay whenever it suits them—even on their smartphone in the supermarket checkout line—they will likely pay faster, reducing your accounts receivable.

Choose a payment processor that is PCI compliant to adhere to the stringent information security standards (PCI stands for payment card industry compliance and is a set of requirements for processing, storing, and transmitting credit card data).

Automatic backups

Advanced data security technology ensures a secure backup of your files every few hours. This means you never have to worry about losing your documents and all of the hard work you put into them. Data encryption and multi-location storage ensure increased security and maximum redundancy so that your files are available whenever you need them.

Complete your firm's security plan with a secure file-sharing and eSignature solution

Comprehensive data security is critical to your firm's success. Not only does it ensure regulatory compliance, but it also helps you cement client trust.

No law firm data security plan is complete without secure file-sharing and eSignature tools. Fortunately, CosmoLex's LexShare and LexSign integration makes it easy.

Our solution allows you to streamline your firm's operations and deliver seamless client experiences by enabling you to send files and signature requests via a secure email link. There's no need to juggle applications or log into a portal. CosmoLex gives you document and file-sharing convenience with one secure click. These solutions offer multiple layers of security thanks to bank-level encryption and knowledge-based authentication (KBA), which provide a deep security level for clients' data.

Schedule a free demo today to see how CosmoLex can help you simplify client data security for your firm.