2026 Law Firm Data Security Guide: How to Keep Your Law Firm Secure

Written by Gavin Miller

Law firm data security should be a top priority for any practice. After all, clients trust you with their most confidential information.

Since clients entrust lawyers with so much of their sensitive data, law firms make prime targets for cybercrime. According to the *ABA Cybersecurity TechReport*, nearly 30% of law firms have experienced a security breach. You don't want your firm to become part of that statistic.

And, while lawyers are increasingly harnessing artificial intelligence (AI) to help them work more efficiently, cybercriminals are also using the technology to augment the scale, power, and creation of cybercrime threats like AI-assisted hacking, password cracking, and ransomware attacks.

So how do you mitigate your firm's risk of data breaches and keep your clients' data secure? As a legal professional, it's crucial to stay up to date with the latest legal technology. But, with technology constantly evolving, where do you start?

Here, we'll outline the fundamentals of law firm data security in 2026. Read on for an overview of best practices for keeping your firm's data secure, a summary of your ethical and regulatory obligations when it comes to tech, a look at the risks and rewards of cloud-based legal software, and resources that can help level-up the data security at your law firm.

Collect client payments with ease and transparency, without third-party integrations. Streamline your billing today with Clio Payments and focus more on your practice, and less on paperwork.

Law Firm Data Security 101

Let's start with the basics. These are the essential things you need to know about law firm data security in 2026.

What is a law firm's data security risk?

Failing to keep data secure is more than just a huge risk for you and your firm. Data security failures can also have incredibly negative consequences for your clients.

To hackers and criminals, law firms are remarkably attractive targets. Valuable information—like trade secrets, intellectual property, merger and acquisition details, personally identifiable information (PII), and confidential attorney-client-privileged data—draws the ill-intentioned to your firm.

Despite these risks, law firms are obligated to protect their clients' information. If criminals penetrate your firm's security, the consequences can be extensive—ranging from minor embarrassments to serious legal issues. This includes:

- **Compromised communications** due to phished or compromised email accounts
- **Inability to access firm information** because of ransomware (i.e., where hackers encrypt files and demand payment to restore access)
- **Public leaks of personal or business information** (e.g., on social media)
- **Loss of public and client trust** in your firm
- **Malpractice allegations and lawsuits**

According to IBM's *Cost of a Data Breach Report 2025*, the average cost of a data breach for professional services firms (including law firms) is $4.56 million. This price tag makes prevention a far smarter investment than recovery.

The *Legal Trends Report*reinforces this urgency. With 79% of legal professionals now using AI and growing firms adopting technology at significantly higher rates, ensuring your tech stack is secure has never been more critical.

What are law firm ethical and regulatory obligations?

Ethically (and professionally), it's your duty to protect client data and to disclose your error if a breach does occur.

According to the American Bar Association (ABA) Rule 1.6: Confidentiality of Information, lawyers should "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

The ABA has also released several ethics opinions (such as Securing Communication of Protected Client Information and Lawyers' Obligations After an Electronic Data Breach or Cyberattack) that provide guidance for lawyers on how to address cybersecurity.

To comply with ABA obligations, you must make reasonable efforts to protect your firm's data. This could include implementing a cybersecurity plan, securing your mobile devices, improving communication practices through email, vetting legal tech providers and enabling two-factor authentication.

It's also important to consider these ethical responsibilities and best practices when adding legal technology to your firm's toolkit. In many cases, legal technology can help you meet your regulatory obligations by better protecting your data, and therefore client data, via streamlined processes (with less room for manual error), enhanced security infrastructure, and encryption.

HIPAA, GDPR, CCPA, SHIELD, and state-specific breach notification laws

Data security laws can vary by location. It's your firm's responsibility to understand your legal responsibilities in the event of a breach.

- **HIPAA**: The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires healthcare providers and "business associates" to protect protected health information (PHI) from inadvertent disclosure. Since law firms are considered business associates, they must comply with HIPAA when handling PHI on behalf of their clients. Check out our blog post on understanding HIPAA compliance for more information.
- **GDPR**: The General Data Protection Regulation (GDPR) requires enhanced protection of personal data belonging to EU individuals. While GDPR primarily applies to firms in Europe, its regulations could affect your firm, as many US states have enacted GDPR-inspired privacy laws. So, it's a good idea to learn more about GDPR.
- **CCPA**: The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), requires enhanced protection of personal data for California residents and gives consumers additional privacy rights.
- **SHIELD**: Similarly, New York has introduced the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which introduces a requirement for companies to develop, implement, and maintain "reasonable safeguards to protect the security, confidentiality, and integrity of private information" of New York residents. The SHIELD Act also enhanced New York's existing data breach notification requirement (already one of the strictest in the United States).

Learn more about state-specific data breach notification requirements.

What to do if your law firm is hacked

Of course, no one wants to believe their law firm could be hacked. Unfortunately, because of the valuable documents lawyers keep on hand, law firms are prime targets. Hackers might intend to steal your clients' data to sell it to third parties. Or, in rarer cases, they could opt to hold the information hostage until a ransom is paid.

Your firm should have an incident response plan (IRP) for these situations—though, hopefully, you'll never have to use it. Below is a good starting point when it comes to creating an IRP checklist:

- Contain the damage and begin any recovery protocol
- Connect with a data breach expert
- Notify your insurance provider (and if you don't already have cyber security insurance, check out our post on cyber security insurance for law firms)
- Report the incident to law enforcement
- Ensure all third parties are notified
- Make compliance a top priority

It's important to review and update your IRP regularly to avoid making a bad situation worse. You can run your checklist by an IT consultant as they might have additional recommendations.

11 best practices for protecting your law firm's data

There's no single way to lock down your law firm's data. Instead, consider a defense-in-depth for data security that employs numerous checks and takes advantage of the latest legal tech. Mac users can start with these security tips; then, for whatever systems you use, consider these best practices for your firm's security.

1. Create and implement a data security policy at your firm

A surprising majority of security issues begin with simple user error—not tech failures.

- Make a clear, easy-to-follow plan for data security and share it with everyone at your firm.

- Educate employees and enforce procedures such as using two-factor authentication for logins, only using apps vetted by the firm, or a Bring Your Own Device (BYOD) policy for employees using their own devices.

2. Continuously train staff on mitigating data risk

Don't assume that everyone knows how to spot and avoid a phishing email. Open a dialogue and continue to train employees to avoid accidental user errors and promote law firm data security best practices. As part of your law firm's cybersecurity protocols, require training upon hire and periodically (usually once a year) thereafter.

Resources like data privacy CLEs can also help your firm understand risks and implement solutions to control them.

3. Use strong passwords

Always. Is your password simple and guessable, like a birthday or—please, no—"123456"? Do you use the same password for every login? If so, you're an easy target for hackers.

- **Use a password manager:** Password managers offer an easy and secure way to generate, store, and autofill unique, complex passwords. These tools encrypt your credentials, helping to safeguard access to case files, client communications, and cloud-based software from unauthorized users.
- **Create better passwords**: For increased password security, go for something complex and long. Use a password management tool to help ensure passwords remain secure and simplify password management (no more having to memorize or write them down—please don't do that last part).
- **Enforce strong password rules**: Some legal tech software, like Clio, feature password policy settings that keep your passwords in line by requiring strong passwords.

4. Encrypt, encrypt, encrypt

Don't overlook this simple yet highly effective measure. Encryption translates your data—whether stored in an email, a local hard drive, or in the cloud—into a coded format that requires a key or password to access it.

- Keep an eye out for applications that will take care of encryption for you. For example, Clio applies in-transit and at-rest encryption using industry best practices (such as HTTPS and TLS) to ensure your firm's data is stored and transmitted securely. Clio's web interfaces are also verified by DigiCert, a trusted certificate authority.

5. Secure your communications

One of the primary ways for hackers to intercept your data is through your communications. As part of your firm's data security plan, review any vulnerabilities across your communication channels and look to mitigate them.

For example, you can encrypt your firm's emails (Trustifi, which integrates with Clio, offers an email encryption security solution.) You may also want to look into communication apps like Signal, which offer end-to-end encryption across multiple messaging methods.

6. Consider access control

Not everyone on your staff needs access to everything. Be intentional about granting permission to view specific matters, and enforce the principles of Least Privilege and Need to Know.

Clio's role-based permissions make this easy. You can restrict visibility to sensitive case information to specific users, ensuring confidential client data stays protected even within your own firm.

7. Conduct regular reviews

It's easy to overlook weaknesses in your law firm's data security if you don't take the time to review it. Conduct regular audits (you could build this schedule into your firm's data security policy) to identify and address law firm cybersecurity and data risks. This includes things like ensuring former employees no longer have access to legal files or ensuring controls such as anti-virus software and firewalls are operating effectively.

If you're looking to take your law firm's data security and privacy to the next level, consider data privacy certifications. Programs like ISO 27001 certification for law firms can not only ensure you have adequate protocols in place but are also enticing to current and prospective clients.

8. Vet vendors carefully

While data security ultimately falls under the ethical responsibility of lawyers, legal technology can definitely help make this easier (or harder). To ensure your provider will do you more good than harm with your data, carefully vet potential vendors. We recommend using Clio's Cloud Computing Due Diligence Checklist.

When evaluating AI-powered legal tools, pay special attention to how providers handle your data. With Clio's Intelligent Legal Work Platform, your firm's data is never used for AI model training, and all AI capabilities operate within Clio's SOC2 and ISO27001-certified security infrastructure.

9. Plan for the worst

Even while actively working to prevent breaches, you need to know what you'll do if one occurs—before it happens.

- **Create a plan for what to do in the event of a data breach**: Detail what needs to be done immediately in terms of communication, changing passwords, and reporting (to impacted individuals or regulatory authorities) if there is unauthorized access to your data. The plan should also specify what your firm should do if a malpractice claim is filed. Also, consider including any guidance provided by the ABA concerning your ethical obligations.
- **Test the plan**: Data breaches shouldn't be left up to theoreticals in the event of an issue.

You should also prepare for what to do in the event of a disaster to ensure your law firm can continue to operate effectively.

- **Create a disaster recovery/business continuity plan**: Include considerations for items such as defining critical systems and equipment, identifying appropriate tools/procedures (e.g., backups, remote sites, or cloud providers), and developing communication plans. Also, consider any guidance provided by the ABA (such as Ethical obligations to clients in the wake of a disaster).
- **Test the plan**: Find out what works (and what doesn't)!

10. Bump up your law firm's mobile security

With more and more legal work done remotely, there's increasingly a need for mobile law firm data security. Secure mobile apps take much of the heavy lifting out of the process (for example, Clio's mobile app for lawyers allows you to access your firm from anywhere). But your smartphone and laptop, in general, might also need a security makeover.

Secure your phone, laptop, and other mobile devices with steps like:

Enable encryption

While having a lock-screen password on your laptops and mobile devices is a first (essential) security measure, it won't protect your data if someone gets a hold of your password. Enable encryption on your mobile devices to scramble sensitive data for unauthorized users and to enhance security.

Here's how to encrypt your iPhone or your Android device.

Set up two-factor authentication

Even strong passwords can be compromised. Two-factor authentication (2FA) adds a critical layer of protection by requiring both your password and a second verification step—like a code sent to your phone or generated by an authentication app.

Why this matters for law firms: Lawyers are responsible for safeguarding sensitive and privileged client information. Enabling 2FA drastically reduces the risk of unauthorized access, helping your firm meet ethical duties and cybersecurity best practices. In many jurisdictions, taking "reasonable precautions" to protect client data is a compliance requirement—and 2FA is a simple, effective way to meet that standard.

Built-in protection with Clio: Legal tech platforms like Clio offer easy-to-enable 2FA settings across all user accounts. This ensures consistent, firm-wide security without slowing down daily workflows.

Bottom line: If you're not using 2FA, you're relying on a single point of failure to protect your firm's most valuable data. For a profession built on trust and confidentiality, that's a risk you can't afford.

Learn how to set up two-factor authentication for your Clio account.

Backup firm data to secure servers

Whether you lose your device or you're the target of a ransomware attack, it's smart to regularly back up your firm data to a secure, encrypted location so you'll still be able to access most of your data.

One of the benefits of using cloud-based software is that backups are taken care of for you (more on this below) and support any incident response and/or business continuity plans you develop.

Keep professional and private accounts separate

Don't risk mixing confidential professional communications with personal ones. By using dedicated apps for your professional work, you can keep these two worlds apart.

Have a plan for lost or stolen mobile devices

If you lose (or someone steals) your smartphone, what's the first thing you'll do?

From having a way to locate a missing device (like Find My Support for Apple devices or Google's Find Your Phone), to knowing how to suspend service or disable your device remotely, it's important to make an action plan before you need it.

Make sure you have full disk encryption on your laptop as well so you know your data won't be compromised if your laptop is stolen or lost.

11. Train your clients

Clients often don't realize their actions may not be secure. Yet, law firms bear the risk when clients expose details, like banking information, to scammers. To prevent this risk from blowing up into trust account errors and payment disputes, lawyers need to train their clients, from their initial conversation, on what methods of communication are most secure and how to use them.

A client should, as part of retention, learn:

- Who to expect will be contacting them
- What methods of communication will be used between lawyer and client
- What steps clients are expected to take to help preserve confidentiality
- How to report anything that deviates from this discussed training

This means that a law firm should show their client how their client portal functions and walk them through logging in and creating a password **before the end of your first meeting**. Set yourself and your clients up for secure communications from the start.

For a universal security checklist and a phased plan to work through it, see *Your Security & Compliance Roadmap*.

Tools to make law firm cybersecurity simpler

Even if you know that data security and privacy are vitally important to your law firm, there's still the potential for you to overlook something, especially if you handle a lot of data.

After all, the majority of lawyers are working overtime to get everything done. According to the *Legal Trends Report*, lawyers bill just 2.9 hours of an 8-hour day—which means important issues like data security could slip through the cracks.

Luckily, in an era where some technology can instill fear, you can also use tech to combat risk and make it easier to protect your firm's data. Here are a few tools to consider:

Signal: For safer communication

Communication is key, but sending unprotected messages can put data at risk. The Signal app—available for Android, iPhone, or your desktop computer—lets you send secure, high-quality, end-to-end encrypted communications (including group, text, voice, video, document, and picture messages) anywhere in the world.

Another bonus? Signal is free.

There are plenty of other communication options in the Clio App Directory as well.

As a reminder, law firms should always do their own due diligence and choose a tool that is best for their firm's needs.

Clio: For safer legal software solutions

Clio's legal software takes protecting your clients' information (and your firm's data) seriously, with security measures designed to help you stay safe and compliant.

Clio's advanced product features and controls work to secure your data through features like:

- **Role-based permissions**: Visibility into sensitive case information is restricted to specific users at your firm.
- **Password policies**: Clio's password policy settings allow you to enforce strong passwords and regular password resets at your firm.
- **Session/activity tracking**: By logging the IP address of every login to your account, Clio helps you keep an eye out for suspicious account activity.

- **Two-factor authentication**: Enhance login security by verifying user identities via their mobile device.
- **Login safeguards**: Is someone trying to guess your login? Clio locks your account for some time—automatically—after too many failed login attempts. A secure client portal also keeps communications encrypted and secure.

Learn more about Clio's industry-leading security.

Is the cloud secure enough for law firms?

Cybersecurity for law firms requires heightened responsibilities for ensuring data security and privacy, and cloud-based software can be a powerful way to get your firm in order. Indeed, in recent years, cloud software has become increasingly more secure than the data security provided by traditional servers in many ways.

While certain inherent risks come with handling sensitive client data in the cloud—such as the potential for data breaches—reputable cloud service providers offer security measures to mitigate risk.

And, though new security risks and considerations will emerge, investment in measures to keep digital information safe is growing. According to Gartner, worldwide spending on security and risk management continues to increase significantly year over year—projected to reach $240 billion in 2026—a trend that shows no signs of slowing.

5 Benefits of the Cloud

By moving to legal cloud computing services, your law firm can likely benefit from the following:

1. **Improved security**: When used appropriately, reputable cloud-based solutions are secure. Increasingly, using the cloud can improve your firm's security by taking advantage of built-in security measures. For example, you can use dedicated security teams, regular security tests, and more that providers invest in.
2. **Easier software updates**: Instead of wasting time and money manually updating your team's on-premise software, you can benefit from regular, automatic software updates from cloud providers.
3. **VPN redundancy**: The cloud lets you work from anywhere, with secure access to your firm's information—without needing a VPN.

4. **Enhanced compatibility**: Cloud-based software companies make it simple to connect with other tools to get the most out of your applications. For example, the Clio App Directory features over 250 available apps to help you customize and streamline your workflows in Clio.
5. **Fewer IT requests and costs**: Quality cloud-based software providers offer top-tier support—like phone support, live chat, and a knowledge center—to all users. These types of support features mean less time and budget spent on resolving basic IT questions from your team. And, with cloud providers reducing the need for on-premise servers and hardware, you'll save money on storage and hardware maintenance.

Security best practices for legal cloud-based services

The cloud offers secure, useful options to help your law firm run more efficiently. However, not all cloud providers are the same. To ensure your cloud services are secure, you need to effectively vet providers and prevent user errors.

When considering legal cloud-based providers, it's important to ask, at minimum, the following:

- **Do they have a security team?** A dedicated, experienced security team indicates that cybersecurity is a priority.
- **Are they compliant?** Cloud providers should advertise their compliance with requirements like the Payment Card Industry Data Security Standard (PCI DSS) and laws such as GDPR and CCPA.
- **Do they conduct automated security scans?** For example, Clio undergoes regular security audits and certifications—including SOC2 and ISO27001—to help ensure products are protected from malware, vulnerabilities, and other online threats.
- **Do they offer an uptime guarantee service level agreement (SLA)?** An SLA speaks to the minimum level of service provided by a company to a customer in their contract; cloud providers should provide a percentage guarantee for uptime. This is the amount of time that the cloud service provider is accessible to end users.
- **Do they encrypt data both in transit and at rest?** Providers should protect sensitive data both while it's in motion and while it's stored or archived.
- **Are they recommended by bar associations and law societies?** Approval and recommendations from legal associations indicate industry recognition for high-security standards.

- **What security-focused features do they promote?** What other measures does the provider take to help ensure enhanced security with their software? You can see an overview of the security measures Clio provides here.

Final thoughts on data security and privacy for law firms

What should take priority when it comes to data security for your law firm? Start analyzing and improving your data security as soon as possible. It's always better to be proactive. You'll avoid the negative consequences of a cyber attack or data breach.

Protecting your clients and your law firm's data is more than just a good thing to do. It's ethically and professionally critical to your role as a lawyer. Understanding your responsibilities and best practices can help mitigate your risk of data breaches. And some of the latest legal technology can take your security even further while also improving your firm's overall efficiency.

Clio provides industry-leading security across your entire practice—from case management and client intake to document automation. With encryption, two-factor authentication, and SOC2/ISO27001 certifications built in, you can focus on serving clients while Clio protects your data. Book a demo today.

Frequently asked questions

Are data security risks high in law firms?

Data security risks are inherently high for law firms, as law firms routinely handle valuable and sensitive information like trade secrets, intellectual property information, merger and acquisition details, personally identifiable information, and other confidential data. Law firms also have certain ethical and professional obligations to ensure the safety and security of this sensitive client data.

Do law firms need cybersecurity?

Cybersecurity is essential for law firms to safeguard sensitive and confidential client information, which in turn allows lawyers to meet their ethical and professional obligations for data security. According to the ABA's Legal Technology Survey, 60% of firms have implemented formal cybersecurity policies. But phishing and ransomware remain major threats, which makes ongoing vigilance essential.

About Clio

Clio is the global leader in legal AI, powering legal work across the profession, from law firms of every size to corporate legal teams, government agencies, and courts. Its Intelligent Legal Work Platform unites the business and practice of law, connecting the people, information, and processes behind legal work. Clio's AI brings the context together with legal sources drawn from Clio Library, a growing collection of more than one billion legal documents. Over 400,000 legal professionals in more than 130 countries rely on Clio to run their legal world. Learn more at www.clio.com.