Data Security in the Cloud: What You Need to Know

Cloud-based legal software has become a popular choice for law firms because it's cost-effective, accessible, and easier to maintain than on-premises options. While these perks are highly desirable, many managing partners still have plenty of questions about one hot-button issue: data security.

If you find yourself wondering:

- What threats should my firm be on the lookout for?
- How common are breaches of legal information stored on the cloud?
- What measures do software providers take to protect client information?
- Is cloud-based software a smart security option for my law firm?

...keep reading!

Data security, the cloud, and you

As an attorney, you know how crucial it is to maintain the confidentiality of your clients' personal information. Your clients are counting on you to keep their private financial and legal information secure. Breaching that trust can have serious consequences—including damage to your reputation, legal liabilities, and repercussions from the national and state bar association.

With so much at stake, it's only natural to feel concerned about data security in the cloud. Rest assured: with the right software provider and team training, cloud-based software can actually improve data security.

Common cloud-based legal software threats

Cloud-based software providers like TimeSolv implement multi-layered security measures to protect sensitive information. Even so, the more you know about different types of security threats, the better prepared you'll be to take a proactive stance on data security at your legal practice.

From payment information and case details to legal strategies and intellectual property, your law firm manages a lot of sensitive data—and that data is extremely appealing to hackers who are trying to commit identity theft, fraud, or other crimes that involve accessing, selling, and/or using sensitive personal information.

Here are some common types of data breaches and cybersecurity threats every attorney who uses cloud-based software should be aware of.

Malware attacks

Malware is a type of software that damages or disables computers, cloud networks, and the information contained in them. Hackers try to use malware to steal data, damage files, or even take control of other software.

Phishing attacks

With phishing attacks, hackers send emails or other messages that look like it's from a legitimate source as a way to trick legal staff into revealing sensitive information, such as passwords or proprietary company information.

Insider threats

Sometimes, individuals who are authorized to access legal cloud-based software willfully abuse their access to commit identity fraud or theft. Even when an insider threat may seem like an isolated incident, your entire law firm could face consequences for failing to protect client information.

Accidental compliance violations

Not every cloud-based software is designed to uphold the strict regulations that law firms are subject to—particularly when it comes to client data. Even if you had nothing to do with a cyber attack at your firm, you will still be held liable, which can result in fines, penalties, and even losing your license to practice law.

How cloud-based software protects sensitive data

While these threats can sound intimidating, they're actually similar to tactics used to attack traditional legal software. The plus side is that cloud-based options offer more robust security measures for protecting client data.

Centralized data storage

With traditional methods of data storage, it's common for the same sensitive client information to be stored on multiple computers that need to be individually updated and monitored for security threats.

On the other hand, when sensitive data is consolidated into one location, such as a trusted cloud-based legal software, you gain better control over who can access it.

And the fewer people who have access to personal details like social security and bank account numbers, the better. That's because even when no insider threats are present, legal team members who are aware of this information could be targeted by phishing schemes.

TimeSolv
by profitsolv
How to Create a Paperless Document Management Workflow for Your Law Firm
LAW
LAW

How to Create a Paperless Document Management Workflow for Your Law Firm

To provide your clients with the best value possible, consider setting up paperless document management workflows.

Don’t know where to start? Consider this your step-by-step map to creating a more efficient, eco-friendly law firm.

Download our free guide to create a paperless document management workflow for your law firm today!

Get your free guide

Monitoring for insider threats

Cloud-based software providers continuously monitor their systems for unusual activity, which can help you identify and respond to insider threats quickly. If a member of your legal team interacts with client information suspiciously, restricting their access until the matter is settled takes only a few clicks.

Regular security updates by dedicated security professionals

With cloud-based software, the providers—not your legal team— are responsible for staying up-to-date with the latest security patches and updates. This reduces the burden of internal IT work while also offering continuous protection from malware attacks and data breaches.

Compliance features

There's a reason that legal firms are under such strict regulatory requirements when it comes to client information. Violating them leads to costly fines—or worse.

By providing features that help law firms comply with regulations, such as data encryption and secure client portals, cloud-based software like TimeSolv can help your firm avoid the consequences of non-compliance.

Choosing the right cloud-based legal software provider for security

Not every cloud-based software provider follows the same security protocols. When it comes to choosing the right legal software for your firm, take the time to find a provider who takes your clients' sensitive information as seriously as you do.

While you don't need to be an IT expert, it's important to look for these key features in any legal software you're considering:

Reputation

Every cloud-based software provider claims to value security, but don't just take them at their word. Instead, look for customer reviews and ratings. A strong reputation can be an indicator of a reliable and trustworthy provider.

If users are complaining often online about missed updates or security breaches, it may be best to seek out other options.

Security features

At a minimum, any legal cloud-based software provider you consider should have firewalls, antivirus software, and intrusion detection and prevention systems in place to protect your client's data.

It's also wise to verify the quality and availability of these features before making your final decision. Do they cost extra? Are they up to date with the most recent threats?

Encryption

In simplest terms, encryption "scrambles" important information so that any unauthorized party who accesses it won't be able to understand it easily. All data your law firm sends through the cloud should be transmitted using highly encrypted 256-bit SSL, both in transit and at rest.

Thousands of law firms trust TimeSolv to protect client data

And for good reason.

TimeSolv has a reputation for taking security seriously. In addition to monitoring and upholding all of the American Bar Association's recommendations for keeping client information secure, TimeSolv is also compliant with SSAE-16 (formerly SAS 70) and SOC 1, SOC 2, and SOC 3 compliance reports, as well as being ISO 9001 certified. We are also PCI DSS compliant.

In other words, your data is in good hands. We recognize that you don't have time to wait for updates, but you also can't afford to skip them. So, we provide you with almost 100% uptime, so you never need to sacrifice productivity for security.

To learn more about how TimeSolv helps your firm prioritize data security in the cloud, start your free trial today and speak with a product expert during the included one-on-one training!