Legal Data Compliance: Understanding Key Regulations for Law Firms

Law firms amass sensitive client data and confidential information, an appealing reward for a sophisticated cyber attacker. According to the 2022 ABA Cybersecurity Tech Report, 27% of law firms experienced a security breach.

Law firms need to be proactive about data security so they don't become a statistic. Learn about your ethical responsibilities to cybersecurity and how you can mitigate your firm's risk of a cyberattack.

American Bar Association (ABA) Data Compliance Rules and Regulations

Lawyers have a professional and ethical responsibility to protect client data and disclose a breach if it occurs. According to the ABA Rule 1.6: Confidentiality of Information, lawyers must "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 also has several Ethics Opinions that guide lawyers on how to address cybersecurity:

- Securing Communication of Protected Client Information
- Lawyers Obligations After an Electronic Data Breach or Cyberattack

Data Compliance Regulations Your Law Firm Should Know

Data security laws are complex and can vary by location, especially for law firms that may handle clients in different locations or with different types of sensitive information. Here are some data compliance regulations your law firm needs to know.

General Data Protection Regulations (GDPR)

In 2018, Europe introduced a unified data protection law, GDPR, for businesses handling personal data. This law requires enhanced protection of personal data for EU individuals. While this only applies to companies in Europe, the regulations could impact a US law firm. It’s best to learn about GDPR and stay compliant.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal law requiring healthcare providers and business associates to safeguard protected health information (PHI) from accidental disclosure. Law firms are considered business associates and may have access to medical records for cases, so it’s essential to comply with HIPAA when handling PHI for clients.

California Consumer Privacy Act (CCPA)

In 2020, California introduced CCPA to mirror GDPR and require enhanced protection of personal data for California residents. Law firms that operate in California or have California-based clients must be compliant with CCPA.

Stop Hacks and Improve Electronic Data Security Act (SHIELD)

Like California, New York introduced SHIELD to safeguard personal data. This act includes a requirement to implement reasonable security safeguards for any business in possession of the personal data of New York residents. This is in addition to the state's existing data breach notification requirement, which is one of the strictest in the country.

Federal Trade Commission (FTC) Act

The FTC Act allows the FTC to prosecute businesses for unfair or deceptive acts or practices, including apps or websites that contain misleading information about privacy and security. This rule applies to all US companies regardless of industry and extends far beyond data privacy. One of the toughest aspects of the FTC Act is that the organization issues fines to companies that aren't compliant and continues to levy them until it's resolved.

Best Practices for Data Compliance in Your Firm

Be Proactive, Not Reactive

A reactive approach to mitigate cybersecurity incidents means you're always one step behind. Law firms are a valuable target for hackers, so it's important to take a proactive approach and implement security measures before a cyberattack happens. This not only reduces the risk of attacks in the first place but limits the damage if one occurs.

Create a Security Policy

An unfortunate number of security issues start with user error, not flaws in the tech. Your firm needs a clear, easy-to-follow plan for data security that everyone at the firm is privy to. Educate your employees and enforce best practices like multi-factor authentication (MFA) for logins and only using approved apps.

Train Staff

Despite the best intentions, staff can be a weak link in your firm's data and cybersecurity. Compromised credentials, accidental link clicks, or weak passwords can be an access point for a hacker. Don't assume your employees know how to recognize and report suspicious behavior – train them. Create a culture of cybersecurity and conduct regular training with current staff and new hires to keep everyone on the same page.

Use Tech with Legal-Specific Security Controls

Data security is ultimately the ethical responsibility of your firm, but the law practice management software you use can make this more challenging. Make sure you vet your vendors thoroughly to ensure that they're as committed to cybersecurity as your firm.

The ideal option is working with a law practice management solution that uses legal-specific security controls, including MFA, activity tracking, user permission controls, and secure client communication portals.

Updates in Data Compliance

As high-profile breaches rise, more and more states and jurisdictions are implementing their own data compliance and information security rules. It's possible that there will even be a federal data compliance regulation like GDPR.

There are 15 states that have bills in progress, as well as three that have laws on the books that went into effect this year:

- Virginia Consumer Data Protection Act (CDPA): As of January 1, 2023, Virginia CDPA will protect the privacy rights of state residents.
- Colorado Privacy Act (CPA): CPA will go into effect on July 1, 2023, and grants Colorado residents rights over their data. This act is similar to CCPA.
- Utah Consumer Privacy Act (UCPA): The UCPA goes into effect on December 31, 2023, and offers businesses a little more leeway than other states. It only applies to businesses that target Utah residents, have revenue of $25 million or more, and meet thresholds for data collection.

International regulations are also changing and affecting international markets. South Africa, China, and the United Arab Emirates all passed privacy legislation in 2021, and it's likely that other countries will follow. The US and EU also have a preliminary deal to outline how US-based companies can store the personal data of European residents.

Stay Compliant with Legal-Specific Software

Robust data security isn't a step above any longer. It's an essential part of running a business, including a law firm. With the sensitive information your firm has, it's essential to be proactive in safeguarding data security and mitigating the

risk of a breach with security controls, training, and security-focused law practice management software.