Privacy and Security Roundtable

Join Information Technology and Risk Management experts to discuss risks, strategies, and ethics in today's legal environment.

By Cathy Bryant, Paul Norwood, Ray Mitchell and Adrian Senyszyn

Law firms are increasingly becoming the target for threat actors trying to access the highly sensitive data of the client the firm represents. Threat actors also may be seeking sensitive information about the firm and its employees. This data must be kept confidential. Data privacy and security in law firms means much more than just complying with government regulations and client requirements. The firm's entire team must understand their obligations to protect client data, organizational data, including employee personal data, as well as the risk and consequences of failing to protect the privacy and security of the data.

We will explore four pillars of protecting data and complying with regulations: Assessing Compliance, Privacy and Security Policies, Training, and Incident Response.

To achieve protection of data of the law firm and their clients, the firm must have an organization wide strategy. It does not matter how large the organization is or what type of clients you work with, defining a strategy for securing data is essential. Attorneys receive, maintain, and transmit sensitive data of the firm and clients, which is attractive to cyber threat actors. It is essential that management is involved in the process and provides sufficient funding and resources

for assessing the firm's security and developing a plan to address privacy and security vulnerabilities and issues.

I. Assessing Compliance

To assess the law firm's compliance, firms should first understand the applicable rules and regulations. As attorneys, the American Bar Association (ABA) has developed Model Rules of Professional Conduct that make legal services ethical, efficient and safe.[1] Additionally, there are ABA Formal Opinions addressing data. Opinions 477R[2] and 483[3] describe mechanisms required to monitor for data breaches, implement security measures to stop incidents, notify clients of a breach, and remediate the damage of a breach. The opinions are clear that attorneys need to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[4]

Opinion 483 makes clear that "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach."[5] The opinion further states that "As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach." [6]

There are many other compliance standards that a firm may be required to meet:

- **ISO/IEC 27001** This standard is a specification for an information security management system. It contains a wide range of controls relevant to information security.
- **PCI/DSS** This security standard is intended to help protect cardholder information. Organizations that process, store, or transmit cardholder data are required to be compliant with this standard.

---

[1] Model Rules of Professional Conduct – American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/ (last visited 7/28/22).

[2] ABA Formal Opinion 477R: Securing communication of protected client information, ABA Formal Opinion 477R: Securing communication of protected client information (americanbar.org) (last visited 7/28/22).

[3] ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack formal_op_483.pdf (americanbar.org) (last visited 7/28/22).

[4] *Id.*

[5] *Id.*

[6] *Id.*

- **AUP** This is the agreed procedure created for independent accounting and assessment firms. The AUO is used to evaluate service provider security, privacy, and business continuity controls.
- **HIPAA** There are three HIPAA rules that need to be considered if you receive, maintain, or transmit protected health information (PHI), generally medical records and medical billing records of clients. The privacy rule covers protection of all PHI, written, verbal or electronic. The security rule establishes standards to protect electronic PHI. And the Breach Notification Rule establishes what a covered entity or business associate must do in the event of a security incident to determine if the incident is a reportable breach.
- **NIST SP 800-53** This government publication provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. Private industries may use NIST SP 800-53 as a guide for their own security measures.
- **CMMC** The cybersecurity framework used by the DOD to measure their suppliers' cybersecurity maturity and ensure protection of Controlled Unclassified Information (CUI) residing on contractor networks.
- **SOC2** Certification developed by the American Institute of CPAs (AICPA), issued by outside auditors, which ensures the organization being audited securely manages the data of its clients.
- **Federal Trade Commission** The FTC is the federal agency charged with protecting America's consumers from deceptive practices. Deceptive practices include false advertising, deceptive phone and emails, ransomware and other threats. The FTC also has a breach notification rule and a HIPAA "gap filler."

II. Privacy and Security Policies

Every law firm should have privacy and security policies and procedures. The complexity of the policies will be based on the type of data the firm has, the size of the organization, and the complexity of its network.

If a firm represents covered entities who share protected health information, the firm must meet the three HIPAA rules. The Office for Civil Rights' HIPAA Audit protocol requests "Obtain and review policies and procedures regarding …" nearly 100 times. Law practices should confirm