NAMWOLF

Information Security Program

SUGGESTED GUIDELINES FOR NAMWOLF LAW FIRM MEMBERS

January 2020 Version

Introduction

Law firms are bound by state rules of professional responsibility to maintain the confidentiality of client information. Recent ethical rulings have made it clear that professional responsibility includes the maintenance of information technology systems that protect client data from cyber and other similar means of data theft.

Most recently, ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018) starts with the following observations about current threats:

> "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be."

Clients are increasingly focusing on the information security of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires. Additionally, depending on the client's needs, certain data may also be subject to protection under other federal or international laws, including HIPAA, GLBA, CCPA, and GDPR, just to name a few.

Background and Process

In September 2019, the Chair of NAMWOLF's Board of Directors formed an ad hoc committee to provide guidance, information and education to law firm members on information security requirements, both as their professional responsibility and to meet the increasing needs from companies including NAMWOLF Corporate Partners. The impetus for this review arose from protocols that were being instituted by various companies with respect to their law firm providers, along with other service providers. The committee was chaired by two law firm members and included in-house counsel from several NAMWOLF companies including representatives from the financial services, insurance, telecommunications, retail, and health care sectors. The full committee and a smaller working group met several times from October 2019 through January 2020 to produce the attached guidelines. There was consensus amongst the members that this committee would deliver guidelines designed to help law firm members establish their own protocols, rather than requirements to be imposed on law firms. Additionally, the committee decided on a "maturity model" that progressed from basic recommendations to the optimal. Some of the public resources used by the committee have been referenced below but much of the information in the guidelines is derived from the internal protocols of the companies represented on the committee.

Disclaimer

These guidelines are not intended to be a final or comprehensive guide, but only to serve as a resource for law firm management and their IT support, as they navigate the cybersecurity landscape. It is intended to be a living document that should be updated as our technology environments evolve and new protocols and threats are identified.

Resources

ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack,"
https://attorneygrievances.com/aba_formal_op_483.pdf
ABA Ethical Rules:
https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/
ISO Network Security Standard:
https://www.iso27001security.com/html/27033.html
NIST Cybersecurity Framework:
https://www.nist.gov/cyberframework/framework
COBIT Information Security Free Preview (must pay for this guideline):
https://m.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf
GLBA Compliance and Checklist:
https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf
HIPAA Compliance and Audit Protocol:
https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
PCI DSS Guide and Checklist:
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Guidelines for NAMWOLF Member Firms

LEVEL ONE | BASIC

General Management

Meet ethical obligations under your State Bar Rules and review ABA Guidelines[2]:

- Model Rule 1.1 Competent representation
- Model Rule 1.6 Maintaining confidential information
- Model Rule 1.18 Duty to safeguard client information
- Model Rule 4.4 Duty to protect third party information
- Model Rule 5.1 Reasonable hiring procedures
- Model Rule 5.3 Duty to supervise non-lawyers
- Model Rule 5.7 Reasonable vendor choices/diligence

Identify an individual, committee, or group to be responsible for data protection, cybersecurity and breaches.

Conduct an Inventory and Risk Assessment to identify what data needs to be protected, the location(s), and the threats to those assets.

Establish information security policy and plan identifying risks and controls in place to protect client data.

Network Security

Minimum Recommendations on Policies and Protocols:

- Have all computers and data systems (e.g. servers) protected with secure password management and a minimum password length of at least 8 characters and complexity (special characters, numbers, and/or phrases) (IT/IN).
- Prohibit personnel from storing, sharing, or writing down passwords unless in a secure location.
- Install anti-virus/anti-malware software on computers; configure software to identify and clean viruses and/or malware automatically and to provide notification of the activity.
- Update timely all anti-virus/anti-malware software definitions.

[2] ABA Ethical Rules: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/

- Apply security software updates and patches promptly following their release by applicable software publishers).
- Password protect and encrypt removable devices that contain client information. e.g. DVDs, USB drives, memory cards.
- Implement a Bring Your Own Device (BYOD) policy.
- Prohibit personnel from storing client information on personally owned devices.
- Properly secure hard-copy documents, storage devices, and/or laptops to avoid theft while traveling.
- Utilize a firm-authorized VPN while working remotely or when connecting to public wireless networks.
- Avoid use of free or non-private email account to communicate with or about client data. e.g. Gmail or Hotmail.
- Implement periodic information security training for personnel on phishing, password protection, data protection, document management and information security incident reporting.
- Configure Outlook (or other email software) to allow for easy identification of external emails (different color font or "[external]" added to the Subject line.

Compliance and Monitoring

Establish a security breach reporting protocol identifying one repository for information.

Establish and maintain business continuity and disaster recovery plans with comprehensive recovery strategies to address business interruptions that would disrupt services provided to the client.

LEVEL TWO| FOR DATA SENSITIVE INDUSTRIES (E.g. Financial Institutions/Insurance/Retail/Healthcare)

General Management

In addition to the standards articulated for Level One:

- Implement reasonable information security policies and procedures that are appropriate for the firm's operations, and the sensitivity of information handled, in compliance with standards of the industry that the firm services.
- Communicate in writing the information security requirements to all personnel working on client matters and enforce compliance through periodic internal audits and external assessments.
- Require a periodic review, update, and approval of the information security policy by law firm management.
- Implement a document retention plan.
- Implement reasonable physical access controls to offices, work areas, and computing rooms to limit the exposure of client Information to those with a need to access.
- Implement reasonable physical protections for work papers and documents.
- Establish procedures to verify, including periodic assessments, that all third-party vendors with access to client Information have policies and procedures equivalent to the firm's required levels.

Network Security

Limit a hosted or cloud environment to process or store client Information to only a U.S. based, privately hosted or dedicated cloud environment (e.g., Microsoft Azure, Amazon AWS) that encrypts the client information while at rest.

Establish written processes and controls for managing network and user IDs, including the provisioning, changing, and disabling of accounts.

Establish written processes to control and limit access to system and administrative accounts.

Maintain strong password practices for systems, admin and personnel:

- Require use of unique passwords that periodically expire.

- Lock out passwords after limited number of failed attempts.
- Limit reuse of passwords.

Maintain strong user account practices:

- Disable user login accounts automatically when inactive for more than 90 days.
- Disable login accounts for users within 24-hours of termination.
- Require the use of multifactor authentication for access to client information either on the firms' system or a third party vendor's system.

Use 256-bit encryption or industry standard, (whichever is greater) on all laptops, mobile devices, and any other hardware, device or appliance that contains client Information.

Establish procedures to securely erase or destroy client information stored in all databases, and on all laptops, mobile devices, and electronic removable media prior to offsite maintenance, recycling, resale, reassignment or disposal, and in connection with termination of services for a client.

Establish procedures to disconnect from client networks within 24 hours of notice.

Configure mobile devices with reasonable protections, including device PINs, auto-locking timeouts, and remote wipe capabilities.

Segregate computer networks using industry standard controls (e.g., firewalls) to prevent destruction, loss, alteration, or unauthorized access to systems containing client information

Implement and maintain controls to secure and limit remote access to law firm systems and applications that store client information.

Prohibit the use of public Wi-Fi when connecting to firm servers.

Wireless access points that provide access to client systems must be configured to only permit authorized devices and users to connect

Compliance and Monitoring

Establish an incident management and breach notification plan which includes immediate notification of all clients that may be affected and any other notifications required by applicable law.

Implement periodic exercises, including tabletop exercises and audits, to test the effectiveness of the incident management plan and implement correction of error recommendations.

Engage an independent third-party company to perform periodic audits and tests the firm's information security controls, including the use of penetration testing. Establish a process to resolve any risks or issues that are identified.

Implement an alarm system or other physical security system (e.g. guarding service, cctvs, etc.) to protect all entry points to your facility.

LEVEL THREE| OPTIMAL PROTECTIONS CONTROLS THAT SOME COMPANIES INCLUDE IN THEIR INFORMATION SECURITY REQUIREMENTS

General Management

In addition to the standards articulated for Level One and Two:

- Establish and administer information security training for all employees at least annually. Require retraining if employees move into roles involving the handling of more sensitive client information. Effectively track all training records.
- Perform background checks on all permanent and temporary employees who have access to client data where permitted by law, requiring background checks on employees of any third-party contractors that have access to your firm's network or client data (e.g. your firm's outsourced IT Service Provider). The scope should include, at a

minimum, criminal and financial checks, where permitted by law.

- Implement policies to return or securely destroy documents and work papers, including document productions no longer required for performance under the retainer agreement unless the firm needs to retain documents to comply with document retention requirements or under malpractice insurance or other legal requirements.
- Maintain Cyber Liability Insurance in amounts adequate and sufficient to protect the firm's interests and liability.
- Implement an Access Control Policy on a least privilege and need to know basis (e.g., only the attorneys working on the matters can access the client data for that matter).

Network Security

Segregate client information from other records, even when stored on backup media.

Configure and enforce mandatory Transport Layer Security (TLS), version 1.2 or industry standard (whichever is greater), for all email communication.

Obtain ISO[2], NIST[3], and/or COBIT[4] certification as appropriate to user's systems and type of data handled for clients.

Provide necessary documentation in support of the client's internal and external audits (e.g., GLBA[5], HIPAA[6], PCI DSS[7]) upon request.

Establish procedures for detecting, remediating and, where appropriate, reporting unauthorized or excessive access, copying, or misuse of client information to the company and, with permission from the company, to its customers

Implement phishing testing for personnel quarterly with training.

Allow clients to perform an assessment of data security at the firm and subcontracted parties' facilities.

No storing of company data outside the United States unless given written consent by the client.

Require two-factor authentication and encryption for remote employees and third parties when accessing confidential company data.

Have security and acceptance criteria defined for new and upgraded computers and networks that can access or store data. Must have security and acceptance criteria defined for new and upgraded Computers and Networks that can access or store data.

Maintain an inventory of all applications and systems under the firm's control that are used to store, process and/or transmit data and make the inventory list available to the client upon request.

Prohibit data storage on removable media, including a mobile device or USB memory keys/sticks unless authorized by the person or committee supervising information security and only under monitored circumstances.

Engage auditors and assessors with established experience in a regulated field to conduct reviews of information. security systems that are specific for highly regulated data sets (HIPAA, GLBA, PCI-DSS, etc.)

Encrypt all client data while at rest and in transit.

Prohibit access to tunneling or proxy services (e.g. bit torrent,

Compliance and Monitoring

Engage a third-party to perform periodic penetration tests on externally facing networks.

Run security and threat scans weekly or monthly on all networks and review for vulnerabilities.

[2] ISO Network Security Standard: https://www.iso27001security.com/html/27033.html

[3] NIST Cybersecurity Framework: https://www.nist.gov/cyberframework/framework

[4] COBIT Information Security Free Preview (must pay for this guideline): https://m.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

[5] GLBA Compliance and Checklist: https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf

[6] HIPAA Compliance and Audit Protocol: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

[7] PCI DSS Guide and Checklist: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf