Agents of the SHIELD: Getting Back to Data Privacy and Security

Sandy Coyne, Lori O'Brien, Ellen Samuel

April 19, 2023

Agenda

What is the Shield Act?

Attorney Ethics: Why should you care about privacy and security?

Tales from the Field

What do I do now?

Speakers

- **Sandy Coyne:** Deputy Director of Operations at Legal Assistance of Western New York, Inc. (LawNY)
- **Lori O'Brien:** Incoming Executive Director at Legal Assistance of Western New York, Inc. (LawNY)
- **Ellen Samuel:** Attorney and CIPP/US. Director of Consulting at Just-Tech. Former Supervising Attorney of Intake at Prairie State Legal Services.

What is the New York Shield Act?

NY SHIELD Act

- Signed into law in 2019 and became fully enforceable in March of 2020
- Amended and strengthened New York's 2005 Information Security Breach and Notification Act
- Requires any person or business that maintains private information to adopt reasonable administrative, technical and physical safeguards and expanded security breach notification requirements
- Broadens the definition of private information.
- Expands the definition of breach.
- Expands the scope to any person or business that owns or licenses private information of a New York resident.
- Imposes new data security requirements.

Non - Compliance with the NY SHIELD Act

Civil penalties up to $5000 per violation

$10 to $20 per failed notification

Maximum penalty $250,000

Attorney Ethics

Why should you care about security and privacy?

Attorney Ethics

Your Ethical Duties:

- Rule 1.1 – Competence
- Rule 1.4 – Communication
- Rule 1.6 – Confidentiality
- Rules 5.1, 5.2, and 5.3 – Supervision

ABA Formal Opinions

- ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 2017)
- ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 2018)
- ABA Formal Opinion 498, "Virtual Practice" (February 2021)

Check your state's ethics opinions for best practices!

New York Ethics Opinions

Opinion 1240 (4/8/22)

Topic: Duty to protect client information stored on a lawyer's smartphone.

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Cybersecurity, Privacy and Data Protection CLE Requirement

Experienced attorneys (admitted to the New York Bar for more than two years) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their biennial CLE requirement.

The Cybersecurity, Privacy and Data Protection category of CLE credit has two parts: Ethics and General (New York State CLE Program Rules, section 1500.2[h]).

CLE Program Areas: Awareness and Application, Protecting Clients, Communicating and Obtaining Consent from Clients, Protecting the Law Office, Supervision, Storing, Maintaining and Destroying, Inadvertent Disclosure/Law Office Failure, and Data Breach/Cyber Attack/Cyber Threat


Tales from the
Field

Tales from the Field

- Phishing Email to Finance from employee requesting a change in direct deposit. Process change: Finance now calls the employee to confirm the request is legitimate.
- In 2015 one of our offices was hit with the cryptowall ransomware due to a staff member clicking on a phishing email. We did not pay the ransom and instead had to reinstall Windows on all computers and the Server.
- We have upgraded out Firewalls, Antivirus program. All staff engage in annual security awareness training. We also use a phishing simulation tool that helps train our staff to spot potential threats.

How are we going to pay for this?!

- Our Director of Technology along with guidance from our Director of Operations and Chief Financial Officer creates our technology budget each year. We make sure to budget for replacing equipment on an appropriate lifecycle as well as budgeting for anticipated tech projects that address our needs.
- We are always seeking out new grant opportunities. These can be state, federal or local grant programs that offer specific funding for technology projects and upgrading your IT infrastructure.
- We were fortunate enough to receive a grant several years ago that paid for new servers, switches, routers and computers for all of our offices.
- For LSC funded organizations, TIG grants are a grant resource for innovative technology projects.
- We were awarded a TIG grant to pay for a Learning Management System for technology training

What do I do now?

Implementing the Shield Act

The Shield Act provides a non-exhaustive list of safeguards.

You must implement safeguards that are appropriate for the size and complexity of your business.

If you comply with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act, or New York's cybersecurity requirements for financial services you comply with the Shield Act.

Implementing the Shield Act

Administrative safeguards

- Conduct risk assessments.
- Train employees in security program practices and procedures.
- Designate someone responsible for the security program.
- Carefully select vendors and set safeguards by contract.
- Adjust security programs as the business changes.

Implementing the Shield Act

Physical safeguards

- Assess the risks of information storage and disposal.
- Create systems to prevent, detect, and respond to physical intrusions.
- Dispose of private information within a reasonable amount of time.
- Protect against the unauthorized access of private information at any point during collection, transportation, and disposal.

Implementing the Shield Act

Technical safeguards

- Identify risks in network and software design.
- Identify risks in information processing, transmission, and storage.
- Prevent, detect, and respond to system failures and attacks.
- Monitor and test the effectiveness of system controls and procedures.

How are we in compliance?

- Created a Data Breach Response Policy (Who is responsible to report a breach and who they report it to)
- All offices sit behind an enterprise grade firewall that can easily be managed remotely and all endpoints should have an enterprise grade antivirus
- Encryption for confidential email
- Monitor and proactively manage all equipment and accounts
- All platform we have that hold confidential information has safeguards such as requiring multi-factor authentication
- Security awareness training for all staff as part of the onboarding process and done at least annually
- Frequently assess our risks and vulnerabilities as the security landscape is constantly changing
- Benchmark with other organizations. Hire consultants if necessary to conduct risk assessments

Plans for the Future

- Multi factor across additional platforms (This will increase security but it also means fewer passwords for staff to remember)
- EDR antivirus (This is the new standard in antivirus programs as it can stop malware from spreading to other files and devices)
- MDM platform (We will build out our current mobile device management platform to better control our data)
- VPN requirement (We have many staff who work remotely and will require that they use our secure VPN connection in order to access any of our tech resources)

Top 10 Things You Can Do Right Now

- Identify all of your information systems
- Implement MFA & SSO
- Separate Admin and User Accounts
- Update Your Infrastructure
- Change Default Credentials

Top 10 Things You Can Do Right Now

- Use Your Firewall
- Harden Systems and Devices
- Completely Offboard Users
- Train your Users
- DRBC

Thank You

Sandy Coyne – scoyne@lawny.org

Lori O'Brien - lobrien@lawny.org

Ellen Samuel – esamuel@just-tech.com