NY SHIELD Act Playbook

A readiness guide for nonprofit organizations and small businesses.

866-784-3543 **RoundTableTechnology.com**

RoundTable TECHNOLOGY

Contents

What is the SHIELD Act?

Let's start with the good news. States within the USA are starting to implement privacy regulations to protect our individual data. As individuals, this is good for us. As leaders of nonprofits, small businesses or any entity that collects data as part of doing business, these laws add new responsibilities and potential liabilities.

New York passed the (awkward acronym award winner) "Stop Hacks and Improve Electronic Data Security Act" (SHIELD) Act on October 23, 2019, and the law went into effect in March of 2020[1].

The SHIELD Act is one of the more clearly written of recent privacy laws. Here is what SHIELD requires for compliance as it pertains to cybersecurity:

> *"...reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."*
> https://www.nysenate.gov/legislation/bills/2019/s5575

Note that the word "reasonable" has a specific legal definition with a long history within the legal system (cool fact, one of the people most responsible for the legal "reasonableness" standard was, no joke, named "Learned Hand"). For purposes of "reasonable" cybersecurity measures, the FTC provides this language:

> *"Employing reasonable safeguards to protect the confidentiality, integrity or availability of data given the type, amount and sensitivity of that data in relation to the size, sophistication and capability of the organization."*

This report provides an overview of the legislation, its implications and how you can prepare for SHIELD compliance at your organization.

---

[1] Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), S5575B (2019). https://legislation.nysenate.gov/pdf/bills/2019/S5575B

Does it apply to non-New York organizations?

The SHIELD Act applies to you if you are in possession of private information, most often in the electronic form, belonging to any New York State resident. Further, the SHIELD Act is part of a larger legislative trend toward data privacy started with the European Union implementing the General Data Protection Regulation (GDPR) back in May 2018. California was next, with the California Consumer Protection Act (CCPA). Then in 2019 New York joined the party.

The National Conference of State Legislatures reports that close to cybersecurity 300 bills in 43 different states were either introduced or considered during 2019 and legislation continued to flood state legislatures through 2020, despite the shifting of budgets and resources to Covid. Federal data privacy and cybersecurity legislation is in the works as well. You may think that in this highly partisan political environment it's unlikely federal legislation will pass, but data privacy and security have significant bi-partisan support.

It is wise to assume that we can expect many more policy proposals to be signed into law in the near future. Cybersecurity and data privacy compliance is becoming another aspect of "doing business" in increasingly digital and online environments.

Are there any exceptions?

There is some flexibility in the law pertaining to small businesses. Those with fewer than 50 employees and less than $3 million in annual gross revenue still must comply, but any security program can be made reasonable and appropriate for the size and complexity of the business.

Organizations that are already in compliance with the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act (HIPAA) are not exempt from SHIELD, but are most likely already compliant given the requirements of meeting compliance for those laws.

What constitutes "private information"?

The SHIELD Act is notable for its definition of "private" information and for covering such information not just in the event of a breach, but also as information that must always be protected by an organization's taking "reasonable" safeguards.

SHIELD identifies two types of information, personal and private. Personal information is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such a natural person" in combination with any one or more of the following:

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password or other information that permits access to a financial account
- Account number, credit or debit card number, in cases when the number can be used to access a financial account without requiring any additional security
- Biometric information, including data generated by electronic devices that capture an individual's unique physical characteristics, such as a fingerprint, voice print, iris image, facial scan

Private information also includes a username or email address in combination with a password or security question that provides access to an online account.

The SHIELD Act covers data belonging to any resident of New York State. The organization may or may not be doing business in New York State. What matters with this legislation is that it is a New York resident's private information.

Personal information also includes an organization's employee information. This can be significant because organizations are increasingly relying upon biometric information for human resources purposes, such as accessing restricted areas or IT departments which require biometric authentication to devices.

How is "breach" defined?

The SHIELD Act is groundbreaking in how it defines what constitutes a breach. Under the law, a breach refers to any unauthorized ***access*** to information, not just unauthorized acquisition. The term breach is commonly used to refer to incidents where information is stolen or taken. We hear about big breaches in the news, where hundreds of thousands or millions of accounts -- and private information such as emails and passwords -- are obtained then sold to criminals or used in attempts to gain access to even more valuable or high stakes accounts.

The SHIELD Act expands this definition of breach. A breach applies to any situation where a criminal had access to private information. This includes incidents where a single account may be compromised, providing ***access*** to much more. For example, the SHIELD definition of breached information would apply in a case where an employee of an organization is the victim of a phishing attack, his or her credentials are compromised, providing a cybercriminal with ***access*** to personal information that the organization is storing. The law does not require that the information is obtained and/or copied to another location.

Good faith access to personal information is not considered a breach. Good faith is considered access to information for business purposes or as an agent of the business. Breaches apply to unauthorized access, or access for the purpose of disclosing the information to unauthorized parties. The key here is that law applies to incidents where persons who should not have access to New York residents' personal information are able to gain unauthorized access.

What happens if a breach occurs?

The language of SHIELD is clear, if you expose my data to an unauthorized party, you have to tell me about it. Immediately.

An organization is legally obliged to "immediately" alert all "owners" of personal information when that information was exposed. While "immediately" is not spelled out, a common interpretation is that notification within 72 hours of discovering the breach would be in compliance.

The law clarifies that organizations can use any of the following modes of communication for notifying affected parties:

- Written notice
- Electronic notice,only in cases where the affected party has given permission to receive notifications electronically
- Telephone notification, which must be tracked using a log

In the event that the costs involved in notifying affected parties would exceed $250,000 or that the breach involves more than 500,000 New York residents, then the law allows for substitute modes of notification. Substitute modes include posting of the notification on the organization's website, or notification in state-wide media. Organizations may also conduct mass notifications via email, but only when the breach has not included email and passwords and the affected party has given access to email communications.

The law also requires that the organization notify the State Attorney General within ten (10) days if the incident affects more than five-hundred (500) residents.

If an organization is compromised and does not comply with the notification rules, the Attorney General can issue an injunction against the organization. The organization is subject to fines of at least $5000 or up to $20 per instance of failed notification, not to exceed $250,000. The potential cost is easy to calculate. An organization that maintains personal information for over 12,500 New York residents and fails to meet the notification requirements, is subject to a $250,000 fine.

What is "reasonable" protection?

The SHIELD Act defines three main areas for establishing "reasonable" safeguards:

This is how the SHIELD Act describes "reasonable" protection in each of these areas. As you will see, rather than defining very specific standards, the law provides the following conditions that would comprise what is meant by "reasonable."

What is "reasonable" protection? (con't)

SAFEGUARD 01 *Administrative Safeguards*

One of the biggest threats to personal information and your organization are your employees who have not had cybersecurity awareness training. On the people side of compliance, SHIELD states that reasonable administrative safeguards include implementing a cybersecurity program that:

- Designates one or more employees to coordinate the security program
- Identifies reasonably foreseeable internal and external risks
- Assesses the sufficiency of safeguards in place to control the identified risks
- Trains and manages employees in the security program practices and procedures
- Selects service providers capable of maintaining appropriate safe, and requires those safeguards by contract
- Adjusts the security program in light of businesses changes or new circumstances

SAFEGUARD 02 *Technical Safeguards*

In order to maintain an effective cybersecurity and information protection program you need to establish specific best practices that become part of everyday operations. The SHIELD Act defines reasonable technical safeguards as those that:

- Assesses risk in network and software design
- Assesses risks in informational processing, transmission and storage
- Detects, prevents and responds to attacks or system failures
- Regularly tests and monitors the effectiveness of key controls, systems and procedures

What is "reasonable" protection? (con't)

SAFEGUARD 03

Physical Safeguards

The main focus of the SHIELD Act is the protection of New York residents' personal information. This has clear implications not just for what data that is collected at your organization, but the lifecycle of data that your organization collects and keeps. This includes informal "systems" such as spreadsheets and even word processing documents. Compliance with the SHIELD Act requires that your organization:

- Assesses risks of information storage and disposal
- Detects, prevents and responds to intrusions
- Protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information
- Disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed

How can I prepare my organization?

The first steps to take is to determine whether your organization is covered under the SHIELD Act. If your organization has any two of the following, then you must fully comply with SHIELD:

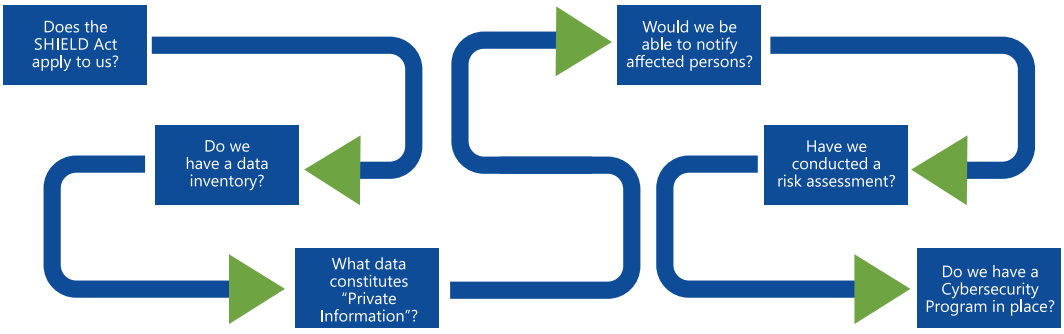
- More than 50 employees
- Greater than $3 million in gross annual revenue
- Greater than $5 million in year-end total assets

If your organization is already in compliance with HIPAA or the Gramm-Leach-Bliley Act, then you are considered already in compliance with SHIELD.

If your organization does not answer "yes" to 2 or more of those criteria, you are ***not*** exempt from SHIELD, but you do have more flexible compliance obligations.

If yes, take RoundTable Technology's online **NYS SHIELD Compliance Checklist**, which provides recommendations based on your level of readiness. The survey also includes links to resources to clarify each of the different requirements.

SHIELD compliance necessitates that you know (and have documented) all of the sources of data in your organization and that you implement a Cybersecurity program that enables you to meet the Administrative, Technical and Physical ***safeguards***.



How can I prepare my organization? (con't)

It is never too soon to get started with conducting a data inventory. This requires that you document the full scope of data collected at your organization. For each data element, identify who owns it, how it is used by different departments and staff and where it is housed. If you use 3rd party cloud-based services, familiarize yourself with their policies regarding cybersecurity and breach protection.

Please note that a complete data inventory includes the "informal" data systems, such as individually owned spreadsheets and documents.

You will need to implement a Cybersecurity program. Outsourced IT providers, such as RoundTable can provide the range of services to meet these requirements. Often this involves starting with a Risk Assessment to understand your organization's gaps and vulnerabilities.

Finally, it is helpful to understand what a SHIELD violation would cost. In the event of an attack, what are the financial and reputational implications of being found in violation of this data privacy law?

How do I respond to a SHIELD audit?

You may have first heard about the SHIELD Act from your financial auditor who is completing a SHIELD compliance checklist as part of this year's annual audit. That is not surprising as the law went into effect in March 2020. However, given that everyone was affected by and responding to the global pandemic in 2020, this law fell under the radar.

If you receive a request for audit, it will most likely come in the form of a checklist. Answer the questions honestly, and use this as an opportunity to take the essential first steps:

- Prioritize your organization's cybersecurity program and strategy
- Conduct an inventory and document all of your data sources

Know that SHIELD will become part of every subsequent audit so these cybersecurity and data management must become part of your day-to-day operations.

Next Steps

RoundTable Technology has created a free **NYS SHIELD Compliance Checklist** so that you can determine how ready you are for SHIELD compliance. The purpose of the survey is informational and your responses are confidential. The survey is based on questions that have been included in audits that we have seen and will familiarize you with the typical sorts of questions that get asked in a SHIELD audit. Please note that there will be variations in the wording and actual questions asked, but this will give you a very good idea of what to expect.

The survey includes resources that explain terms and key concepts associated with the SHIELD Act. As well, the survey points you toward next steps so you can create a SHIELD compliance plan.

***If you have questions about the SHIELD Act**, or if you are interested in RoundTable's Cybersecurity or our Complete program, please give us a call at 866-784-3543.*

RoundTable COMPLETE

Complete = Compliance