

Common Gaps in Information Security Compliance Checklist

DANA B. ROSENFELD, ALYSA ZELTZER HUTNIK & CHRISTOPHER M. LOEFFLER OF KELLEY DRYE & WARREN LLP

This Checklist describes relevant legal obligations and common gaps in information security compliance pertaining to personal information of individuals.

Most companies understand the consequences of security breaches. But how well do they recognize their potential security gaps that could lead to breaches?

Nearly every company collects, stores, handles, shares, transfers and disposes of personal information, including customer information, employee information, business partner information and other personally-identifiable information (PII). In most cases, this personal information is stored electronically in various forms. No security is perfect, and for most companies, the question is not **if** the business will incur a data security breach, but **when**. For recent data on the number of data breaches and their related costs, see *Box, Data Breach Statistics*.

Data breaches involving PII vary, but there are several common types of breach events that can trigger notification obligations and serve as the catalyst for costly investigations and litigation including:

- PII is lost by an employee or stolen by an employee or third party.
- PII is downloaded, copied or accessed by an unauthorized third party.
- PII is used by an unauthorized person (for example, fraudulent accounts are opened or identity theft is reported).
- PII is used by an authorized person (such as an employee) for unauthorized purposes.

To help companies avoid security gaps, improve compliance and prevent costly breaches and sanctions, this checklist describes:

- Relevant legal obligations.
- Common gaps in information security compliance.

LEGAL OBLIGATIONS

To identify gaps in compliance, companies must have an understanding of the applicable legal obligations. In the US, a variety of federal and state laws regulate the handling, storage, use, sharing, disposal and protection of PII. This patchwork of laws presents unique challenges to developing a framework for protecting the various types of PII that the company may handle, including the PII of its customers and employees, as well as responding to legal requirements when a data security incident occurs. Below is a list of the general categories of federal and state privacy and data security laws to keep in mind when reviewing gaps in compliance. For a more detailed discussion of key federal and state privacy and data security requirements, see *Practice Note, US Privacy and Data Security Law: Overview* (<http://us.practicallaw.com/6-501-4555>).

LAWS RELATING TO PROTECTING PERSONAL DATA

Several federal and state laws require businesses to protect PII (including the handling, disclosure, access, storage and disposal of PII).

- Federal laws include:
 - Section 5 of the Federal Trade Commission (FTC) Act (provides general authority for the FTC to prohibit unfair or deceptive acts or practices for all types of information).
 - The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (regulates financial institutions and through contract their service providers).
 - The Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule and Safeguard provisions (regulates the protection and disposal of consumer credit information and the truncation of payment card information).
 - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (regulates certain health care providers and their business associates).

State laws include:

- General consumer protection laws (generally prohibit unfair or deceptive acts or practices involving residents of the state).



- Safeguard laws (regulate the storage, handling and protection of PII, including when sharing with vendors and service providers).
- Social Security number protection laws (regulate the storage, handling and protection of Social Security numbers).
- Disposal requirements (regulate how a business must dispose of PII).

LAWS RELATING TO SHARING DATA WITH THIRD PARTIES

If the company shares any PII with third parties, it may be subject to certain restrictions or disclosure obligations that may arise from a variety of sources, including:

- Federal GLBA and HIPAA requirements (for financial institutions and healthcare providers and the third parties with whom they share PII).
- Promises made to customers and other individuals in privacy policies (for example, statements that the company will not share customer personal information with third parties except under certain circumstances).
- California's "Shine the Light" Law (requires companies to disclose details of third parties with whom they have shared PII for marketing purposes).
- State safeguard laws (may require businesses to contractually require their service providers or other contractors to take certain steps to safeguard PII).
- Industry standards and guidelines. For example, the Payment Card Industry (PCI) Security Standards Council, an international industry organization, requires member banks issuing credit or payment cards to contractually require their merchants to comply with the PCI Data Security Standard (PCI DSS).

DATA BREACH NOTIFICATION LAWS

Most states, and the District of Columbia, Puerto Rico and the US Virgin Islands have enacted data breach notification laws that apply to businesses. In the event of a data breach, the company may be required by law to notify:

- Affected customers or employees.
- State attorneys general or regulatory agencies. For a chart, see *State Agency Notice Requirements for Data Breaches Chart* (<http://us.practicallaw.com/5-501-9110>).
- Credit reporting agencies.

The specific notification requirements may depend on the type of personal information affected and the affected parties' state or states of residency. While there are several common notification obligations across the states, many states have enacted data breach notification laws that contain unique provisions that require a specific response.

Additionally, the company suffering the breach may have obligations to notify business partners. These obligations may arise from contractual relationships with vendors and service providers or from state law requirements if the company becomes aware of a data breach but is not the ultimate owner of the affected information. Each data breach is different and the company's response must be tailored to the unique facts presented by each incident.

For a more detailed discussion of breach notification laws, see *Practice Note, Privacy and Data Security: Breach Notification* (<http://us.practicallaw.com/3-501-1474>). For a model notice letter, see *Standard Document, Data Security Breach Notice Letter* (<http://us.practicallaw.com/3-501-7348>).

WHAT DO LEGAL OBLIGATIONS REQUIRE IN PRACTICAL TERMS?

To effectively comply with the various federal and state data security laws, businesses should (and under some laws are required to) develop, implement and periodically update a comprehensive written information security program. While many businesses develop information security programs to address a specific business function or department, a holistic program that adapts to the changing nature of the business and relevant data security threats is necessary to help prevent data breaches and effectively respond to a breach when it does occur.

In 2014, The National Institute of Standards and Technology published its Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) pursuant to Executive Order 13636. The NIST Framework sets forth a flexible framework upon which businesses can develop their cybersecurity programs and references globally recognized standards for cybersecurity. While the NIST Framework is voluntary and principally directed at critical infrastructure, security experts expect it to be widely implemented and to provide a standard of care of sorts with respect to cybersecurity. Accordingly, companies should refer to the NIST Framework when developing or assessing their security programs.

Generally, as part of its comprehensive written information security program, the company should:

- Review the requirements of applicable laws and regulations as well as industry requirements or standards.
- Ensure that the program is enterprise-wide (a common mistake is to limit the program to the information technology (IT) group).
- Identify the groups and individuals responsible for leadership of the program.
- Identify the types of PII the company collects, stores and shares and where this PII is located.
- Conduct initial and then periodic risk assessments based on possible risks to the security and integrity of PII.
- Set out policies that map out information security requirements, including appropriate administrative, physical and technical safeguards.
- Ensure that the safeguards are actually implemented.
- Implement controls to ensure the program is being followed by employees and contractors.
- Ensure that service providers are contractually required to implement appropriate security measures and oversee and monitor these service providers.
- Include enforcement measures to ensure accountability for violations of program policies and procedures.
- Recognize that the program is dynamic and review, test and adjust the program periodically when the business's practices or laws change (but no less than annually).

COMMON GAPS IN INFORMATION SECURITY COMPLIANCE

GAPS IN SECURITY POLICIES AND PROCEDURES

While a written comprehensive information security program creates the framework for data breach prevention and response, businesses still may suffer a data breach because the program does not adjust to developing needs or is not enforced. Common mistakes in the development, implementation and enforcement of security policies and procedures include:

- Not developing policies in the first place or failing to implement policies.
- Not designating specific employees or groups of employees to maintain and implement the program.
- Permitting the haphazard collection and sharing of PII inconsistent with policy requirements.
- Not updating or modifying policies as the business's information practices or laws change.

GAPS IN INFORMATION STORAGE AND DISPOSAL

To effectively prevent a data breach, the company's data storage practices should be fully understood. Many data breaches can be prevented by conducting an assessment of data storage practices and eliminating common security pitfalls. These pitfalls include:

- Not knowing what PII the company stores and where it is stored.
- Security levels that are inconsistent with type of data stored. This may include the failure to encrypt and/or truncate sensitive PII as required by applicable law or as recommended under industry guidelines (see *Gaps in Technical and Physical Safeguards for Security Systems*).
- Not limiting access to PII to those with a "need to know" that information to perform their duties.
- Retaining PII longer than necessary to carry out the original business purpose.
- Improperly disposing PII that is no longer needed. Companies should keep in mind that some federal and state laws have specific disposal requirements for PII. Disposal of PII should include:
 - shredding all paper files with a cross-cut shredder; and
 - fully wiping all electronic data before discarding or reusing equipment (including when old equipment with information storage capability is sold or released).

GAPS IN TECHNICAL AND PHYSICAL SAFEGUARDS FOR SECURITY SYSTEMS

A business's information security systems may contribute to a data breach if appropriate technical and physical safeguards are not applied. Gaps in technical and physical security extend beyond the IT department and may include systems maintained by human resources or other divisions that manage contractual relationships with third parties and collect or maintain PII.

Common pitfalls related to technical safeguards include:

- Technical security that does not meet legal requirements or appropriate industry or regulatory standards based on the sensitivity of the PII. This might include a failure to encrypt or truncate PII legally required to be encrypted or truncated. This might also include failing to implement or frequently update:
 - logging controls (to track who has accessed PII and when);
 - user authentication (to verify that the person signing into a computer is authorized to access that PII) and password controls;
 - firewalls (designed to block unauthorized users or communications from a computer network);
 - software protecting against viruses and other malware;
 - intrusion detection technology (aiming to identify possible security breaches including third party attacks or internal misuse of a computer or network); and
 - security patches (software designed to fix or "patch" a security vulnerability found in existing software).
- Failure to extend technical safeguards to PII:
 - stored on or transmitted via portable devices (for example, Massachusetts regulations require that, if technically feasible, all PII stored on portable devices (including laptops) be encrypted);
 - housed off-site (including computer back-up copies), collected via a website, accessed through remote systems; and
 - during transmission or transportation (for example, Massachusetts and Nevada laws require encryption of PII transmitted over wireless or public networks).

Common pitfalls related to physical safeguards include:

- Failing to restrict physical access to PII to necessary employees or vendors or service providers.
- Failing to change vendor-supplied and default passwords, or not requiring strong passwords.
- Allowing terminated employees to continue to access records containing PII after employment is terminated or the employee resigns.

GAPS IN ADMINISTRATIVE SAFEGUARDS

Developing a framework to protect PII does not begin and end with the IT and legal departments. The company should examine administrative policies and procedures, as well as informal practices, to ensure that the company is not susceptible to these common gaps that may lead to a data breach:

- Inadequate privacy and security employee training. Companies should institute a culture of data privacy and security awareness from the top down, including periodic training for employees who have access to or handle PII.

- Not monitoring for data leakages or unauthorized use or access. A monitoring program should address data leakage due to:
 - internal and third party e-mail accounts and mobile devices (for example, laptops, smart phones and personal digital assistants (PDAs));
 - remote access systems; and
 - data being physically removed from company premises without authorization (for example, through use of unauthorized USB drives).
- Failing to maintain an accurate and complete inventory of laptops, PDAs and other mobile devices. Companies should ensure it has and enforces a mobile device policy that requires:
 - contractual restrictions on use of these devices by employees, contractors and vendors; and
 - technical measures restricting storing data on, or copying data from, these devices.

GAPS IN USE OF VENDORS AND SERVICE PROVIDERS

Business departments that contract with vendors or service providers should ensure that steps are taken to select appropriate partners and set out a framework that allows the company to monitor and control how the vendor or service provider handles the company's confidential information and PII. Common gaps in this area include:

- Contracts that fail to sufficiently require vendors and service providers to protect the PII the company shares with them.
- Lack of oversight of vendor and service provider practices. Appropriate oversight might include:
 - performing due diligence in selecting vendors to ensure they are capable of maintaining appropriate security measures;
 - periodically reviewing the vendor's privacy and data security policies during the relationship; and
 - requiring audit rights or other disclosure requirements throughout the relationship to keep the company informed of the vendor's current data practices.
- Failure to require the company's own contractors working on-site to be subject to, and trained on, the company's security requirements.

Particular trouble spots with vendors and service providers to be aware of include:

- Handling mobile devices or media with PII.
- Encryption and truncation requirements.
- Transportation or transmission of PII (including over public or wireless networks).
- Risk allocation (including indemnification obligations) for security breaches.

SELF-ASSESSMENT OF THE PROGRAM'S EFFECTIVENESS

An information security program must continually adapt to new business practices and data security risks. Regular self-assessments are important to maintaining an effective program. These self-assessments must be thorough enough to discover potential risks and respond to them before they lead to a data breach.

A comprehensive, appropriate risk assessment must examine the risks relevant to each business division that collects, accesses, stores, disposes of or otherwise uses PII. As part of the assessment, the company should:

- Identify the types of PII collected, including the level of sensitivity, and how such PII (both hard copy and electronic) is:
 - collected;
 - stored;
 - accessed;
 - transferred; and
 - disposed.
- Confirm employees are aware of, and comply with, the company's security policies.
- Identify security controls around all access points to PII, and evaluate whether they are reasonably effective.
- Assess if there is a legitimate business reason for retaining older PII.
- Ensure that PII use complies with company privacy policies.
- Require security audit reports to be a team effort involving representatives from each relevant business division, IT, human resources, legal and senior management.

GAPS IN SECURITY BREACH COMPLIANCE

Even when the appropriate tools are in place to prevent and respond to a data breach, there are several common obstacles that hinder businesses from efficiently and effectively complying with legal and contractual data breach notification obligations and company policies. These missteps drastically slow down the breach notification process creating the risk of delayed notice or non-compliance resulting in sanctions, fines and public relations obstacles. Common mistakes to avoid include:

- Failing to have or follow a written incident response plan addressing how to respond to a data breach.
- Neglecting to involve key participants from all necessary business teams (including IT, the affected business unit (preferably a manager), legal, human resources, public relations or corporate communications and senior management) or share information in real-time.
- Failing to notify affected individuals (including customers or employees) and regulatory agencies in the time or manner legally required.
- Not providing notification to other relevant third parties (for example, service providers may be contractually required to notify their customers).
- Forgetting to document the responsive actions taken by the company or conduct a post-breach review of the incident and implement necessary changes to the program as a result of the review.

For a more detailed discussion of breach notification laws and how to prepare for and respond to a data security breach, see *Practice Note, Privacy and Data Security: Breach Notification* (<http://us.practicallaw.com/3-501-1474>).

GUIDELINES FOR PAYMENT CARD PRACTICES

Businesses that accept credit and debit cards for payment must comply with the Payment Card Industry Data Security Standard (PCI DSS). Specific requirements may vary depending on the payment device used, but set out below are general guidelines for payment card information security.

Do:

- Implement and enforce a written information security program.
- Install and update a firewall that protects cardholder data.
- Assign a unique ID and use a robust password for every employee with computer access.
- Restrict physical computer access to those who "need to know."
- Encrypt cardholder data if transmitting over wireless or open, public networks.
- Use and update anti-virus software.
- Secure company systems and applications.
- Regularly monitor and test networks and systems.

Do Not:

- Use vendor-supplied or default system passwords or common or weak passwords.
- Store cardholder data in company systems in clear text.
- Store magnetic strip cardholder data.
- Leave company systems that store cardholder data vulnerable to SQL injection attacks.

DATA BREACH STATISTICS

NUMBER OF DATA BREACHES AND RECORDS EXPOSED (2012)

While a large percentage of data breaches are unreported, the statistics for 2011 demonstrate that security breaches remain a risk to businesses:

- 614 reported data breaches in 2013.
- Nearly 92 million records exposed.

Type of Entity	% of Breaches	% of Records
General Businesses	34.4%	84.0%
Educational Institutions	9.0%	3.5%
Government/Military Institutions	9.1%	2.0%
Medical/Healthcare Centers	43.8%	9.6%
Banking/Credit/Financial Institutions	3.7%	0.9%

Source: Identity Theft Resource Center.

DATA BREACH COSTS (2006-2013)

Average total cost per incident:

- 2013: \$5.8 million.
- 2012: \$5.4 million.
- 2011: \$5.5 million.
- 2010: \$7.2 million.
- 2009: \$6.7 million.
- 2008: \$6.6 million.
- 2007: \$6.3 million.
- 2006: \$4.8 million.

Source: Ponemon Institute.

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at practicallaw.com. For more information or to schedule training, call **888.529.6397** or e-mail training.practicallaw@thomsonreuters.com.