A Privacy and Data Security Checklist for All

July 2015

Author

Kirk Nahra
Partner
202.719.7335
knahra@wileyrein.com
Twitter: @KirkJNahrawork

Many companies know they have to follow privacy and data security rules. Companies in the health care industry know about Health Insurance Portability and Accountability Act (HIPAA). Financial services companies know about GLB. Some companies know about COPPA or CAN-SPAM.

There are dozens of federal laws, and hundreds (probably thousands) of state laws addressing privacy and data security. Becoming fully educated on all of these laws and how they can apply to a complicated business that deals with significant consumer information is a full-time job, often for a team of people. However, there are certain issues that affect virtually every company, regardless of industry. Here's a quick checklist of privacy and data security topics for any company – and some thoughts about how best to identify and think through your legal obligations.

Employee Data

Essentially, every company has employees. You have personal data about those employees, including (in most cases) their Social Security numbers (SSNs). You also have a wide range of other information about them, including their benefits, their pay, their job performance, and other sensitive or risky pieces of information. You also need to recognize that your employees can create risks as well – in how they perform their jobs, how they protect the personal data that your company maintains, and whether they can be trusted with this information. So, having an effective approach to (1) how personal data about employees is gathered, used, and disclosed; (2) how you will monitor and oversee employee behavior; and (3) effective security practices to control how your employees act is critical. You must understand this data, understand how your employees use data, and what your most significant risks are in this area.

Overall Data Security

Any company that has customers or employees has an obligation to protect the security of sensitive personal data. While there are a series of federal legislative proposals that may create new federal obligations for most companies, the most general set of information security

requirements comes from the Federal Trade Commission (FTC). These rules apply generally to every company. While they are not detailed, they require an important focus on effective security practices, ranging from employee access to disposal of paper records to physical security to protecting information networks.

To meet the FTC's requirements for a "reasonable and appropriate" data security program, the company must:

- Develop and implement a written comprehensive information security program that is appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information at issue.
- Develop a security program that (1) ensures the security and confidentiality of customer information; (2) protects against "any" reasonably anticipated threats to security or integrity of information; and (3) protects against unauthorized access that could result in substantial harm or inconvenience.
- Designate specific employees to coordinate security.
- Identify reasonably foreseeable risks and assess sufficiency of safeguards.
- Oversee service providers by due diligence and requiring contractual security standards.
- Evaluate and adjust its program in light of changes.

These requirements have significant flexibility, but require a thoughtful, proactive security program that stretches across a company's full operations and keeps pace with ongoing changes in both business operations and technological evolution connected to information security. The FTC has just released guidance for businesses addressing these overall data security requirements. The guidance is available here.

Cybersecurity

While the FTC's requirements focus on "data security" and the protection of personal information, most companies also should be considering broader cybersecurity protections. While not precisely a "privacy" issue, cybersecurity risks are growing, visible across wide audiences, and applicable to virtually every company. Effective cybersecurity practices will protect your overall information networks at the broadest level – and therefore will protect how your business operates, and all of the data that you maintain, whether personal data or sensitive corporate information. Every company should be acting in this area – and watching carefully for new federal requirements coming down the road in the short term.

HIPAA

While the focus of HIPAA privacy and security rules is on the health care industry, these rules set out obligations that apply to a large volume of companies across many industries. Your company must consider HIPAA's requirements if any of these categories apply to you:

- You are in the health care business as a health care provider or health plan;
- You contract with companies in the health care business (a service provider to these health care companies);
- You contract with companies who contract with companies in the health care business (and onwards downstream indefinitely); or
- You provide health care benefits to your employees (the broadest and least understood category of requirements).

In addition, there are many companies who must pay attention to and analyze HIPAA's requirements because the companies use or disclose health care information, even if they are not directly regulated by the HIPAA rules. Accordingly, while HIPAA is not an overall privacy and security rule, it covers a large range of companies, many of whom may not be aware of their responsibilities.

Website Privacy Policy

For any company that operates a website, it has now become common practice to develop an appropriate website privacy policy. The detail and challenge for these policies varies significantly based on what the website does and what information is collected. While there is a limited number of laws defining specific responsibilities for these policies, at a minimum most companies must (1) ensure that they do not run afoul of the FTC, by making sure that the privacy policy is complete and accurate; and (2) meet the specific requirements of California's law on website privacy practices, including the core components for such a policy and the recent changes involving "Do Not Track" commitments. The key to these policies is to be accurate and thorough, so that individuals (or others who may be checking) can understand and evaluate your information sharing practices.

Telemarketing/Email Marketing

Most companies do marketing through various channels. For many legislators, regulators, and privacy advocates, marketing (and the use of consumer data for marketing) is one of the "evils" that must be regulated by law.

Marketing activities have been regulated by practice. The Do Not Call laws (including the various federal components and the supplementing state laws) are one of the most successful privacy laws (at least from the consumer perspective), as individuals seem to care about these issues and have in droves signed up for the Do Not Call registries. These issues only affect your company if you conduct telemarketing. If you do, this is a big deal.

On a broader level, the CAN-SPAM law that deals with e-mail marketing has a broader application to a wide range of companies. This law applies to a wide variety of communications, not all of which are obviously "marketing." In addition, this provision applies to both personal and commercial communications, and requires a series of complicated (although relatively modest) steps to comply with the law. Aside from obvious marketers, such as retailers, this law is affecting the business practices of trade associations, universities, professional services firms, and many others. Canada has recently adopted its own version of CAN-SPAM which requires more aggressive front-end consent from individuals. If your company engages in any activity that could be construed as marketing through e-mail, then you must make sure that you are complying with these provisions. You also must evaluate any other marketing practices that you employ, and carefully evaluate how you use and disclose information about your customers.

International

Many companies also need to consider the implications of international data privacy laws. The European Union has led the way on data privacy requirements for many years, and is in the middle of a substantial reevaluation of overall data privacy requirements. More countries add their own laws each year. These laws typically are different from U.S. law. You must pay attention to these international issues – and develop an effective

compliance strategy – if (1) you have employees in other countries; (2) you have customers or vendors in other countries; or (3) you rely on data from other countries. Each of these areas creates compliance risks and obligations. Are you using a cloud vendor? Then the international laws may be triggered. Many companies take a quick look at these issues and decide they aren't relevant. That is often wrong, and can be quite risky. Consider this issue carefully in your privacy and security planning.

Vendors

Virtually every company has vendors. Any vendor that receives any personal information from your company – about employees, customers or others – can create legal risks and compliance obligations. You should have privacy and security contracts with these vendors. You should have a plan for monitoring and overseeing their behavior. You should have an approach to vendor risk management. And you need a plan in the event that one of these vendors has a security breach involving your company's information.

Breach Notification

The last "generally applicable" privacy and data security provision involves the laws in virtually every state addressing notification to individuals in the event of a security breach. While these laws apply (in most situations) to only a limited range of personal information (such as Social Security numbers and credit card numbers), these are pieces of information that are held at least to some extent by virtually every company, at least as an employer. Now states are adding other data elements (such as health care information in California) that expand the reach of these statutes. And, since these laws apply to protect individuals residing in a state, the laws apply to any kind of company, large or small, regardless of industry or geographic location. In addition, there are several federal proposals that are working their way through Congress that may make these requirements applicable at a national level.

These laws, at a minimum, require notification to individuals in the event that their personal information is subject to a security breach (as defined by each law). Some laws require notification to state attorneys general, as well. While typically not required by laws, these notifications often (as is becoming a standard practice) incorporate credit monitoring protection and other protections for individuals. There are certain relatively common terms to these laws, but there also are a wide variety of state specific provisions that turn any breach involving individuals in multiple states into a significant compliance challenge. Because these notification letters typically become public, they also increase the likelihood of litigation or enforcement, as well as adverse publicity. While the explicit goal of these laws is to provide notification to individuals, so that they can take action as appropriate (for example, to protect against identity theft), these laws also have had the effect of improving overall information security practices.

Action Items

So, what do you need to do about these laws? While companies vary in their knowledge of and planning for these obligations, here are some key steps to consider regardless of your level of regulation or preparation.

Do you know what kind of information you have and what happens to it?

Each company has its own privacy/data security risk profile, based on the industries you work in, the kinds of data you have, and the businesses and consumers to whom you provide services. Every company needs to think about the information you have and what you do with it, as a starting point. These steps include:

- Evaluate any place in your company where you collect, store, and disclose sensitive data (especially SSN and credit card information) – this review of SSN usage is the single biggest risk reduction step you can take.
- Pay attention to employee data as well as customer data.
- Can you identify where this information is disclosed?
- Are you paying attention to the right rules?

Then, once you have a sense of the personal data gathered by your company, think about the regulatory requirements for this information and for your business.

- Are you following the various marketing rules?
- Do you collect information from children online?
- Have you thought about your health care benefits program?
- Are you disposing of sensitive information properly?
- Have you told your employees how you monitor them?
- Do you have an appropriate information security program?

Moving beyond privacy issues, companies then must turn to the generally applicable principles regarding information security. These steps are both required by enforcement practices (for all industries) and detailed legal requirements (for certain industries) and protect your company against lawsuits, customer complaints, and business disruption. In thinking about information security:

- Is someone assigned responsibility for data security?
- Do you have documentation for a regulator?
- Does your program encompass paper and electronic information?
- Have you trained your employees on basic information security?
- Do you have appropriate contracts and oversight of vendors?
- Are you ready to act if there is a problem?

All of these proactive steps are designed, at least in part, to reduce the likelihood of an actual problem. One key element of protecting your company is to make sure that if a problem arises, you are prepared to act quickly to reduce potential harm and protect the company and your customers as much as possible. In considering these issues:

- Do you know who is in charge?
- Do your employees know where to go in the event of a problem?
- Do you have a good program to identity and fix problems?

- Have you evaluated the requirements for security breach mitigation and notification?
- Have you considered whether cyber-insurance or other data breach insurance is right for you?

Last, beyond thinking about your own business activities, you also need to think about your business partners, both your customers and your own service providers. Effective compliance is a legal requirement and a business imperative in dealing with potential customers. For your own vendors, service providers create significant risk and must be overseen effectively. Make sure you are thinking about the following points:

- Assess the company's role as a vendor and as a company that hires vendors.
- Develop an "off-shoring" approach.
- Develop a realistic vendor approach for due diligence, oversight, monitoring, and contracting that, for the most part, is "one size fits all."
- Make sure company employees are aware of these responsibilities – and don't take on too much or give away too much.

Final Thoughts

Privacy and data security are not going away. New laws and regulations are placed on the books regularly. Enforcement, while still modest, is growing. Litigation also is growing. And ongoing developments involving the risks and benefits of "big data" present the certainty that the complexity of this environment will continue to grow.

Effective privacy and data security practices are an essential component of the business operations of any business. There is a need for broad understanding of these issues across senior management (and the Board of Directors), and a risk if information practices are not handled carefully and thoughtfully. While the challenges may seem daunting, the most important step is to understand your general level of exposure, and to undertake a creative, thoughtful, and thorough assessment of your privacy and data security activities, so that these growing risks can be managed effectively.