MAY 2010

Privacy Law Alert

from the Privacy and Information Security Group of Poyner Spruill LLP

Seven Questions to Assess the "Privacy Health" of Your Organization

by Elizabeth Johnson

Information about individuals is more readily available now than ever before in history, and its value both to legitimate business interests and to criminals is increasing. Storage options abound, and the trend is to store ever-greater quantities of data on ever-smaller devices, enhancing portability and increasing flexibility for out-of-office access.

The explosion of information's value, availability, and mobility has created a corresponding escalation in risk and compliance obligations with respect to the privacy and security of that information. More than 40 states, the District of Columbia, Puerto Rico, and the Virgin Islands now require organizations to notify affected individuals when personal information has been (or is suspected to have been) subject to unauthorized access or acquisition. Those same laws often also require that government regulators be notified of the breach.

More than a dozen states mandate some form of comprehensive information security, and more than 35 regulate security of Social Security numbers. Relevant to employers' group health plans, federal regulations mandate specific security requirements for protected health information and, more recently, breach notifications for individuals and regulators when a breach of such information occurs. Competing mandates with respect to information disposal, employee monitoring, direct marketing, and online operations also collude to create a dense, intricate, and risk-rich compliance environment.

Full and meaningful implementation of a comprehensive compliance program is the best, if not the only, appropriate response to these considerations. Because both international and state privacy laws generally apply based on the residency of the individuals whose information is at issue, an organization with employees or customers in multiple countries or states will find it necessary to formulate an approach that covers dozens of applicable state laws. Since the laws diverge in terms of scope and substance, synthesizing the requirements is certainly a challenge.

In the face of this complex challenge, it's often best to start simple by getting a high-level feel for the general "privacy health" of your organization. To start, consider the following questions:

Q Have you implemented a comprehensive, written information security program?

Government regulators who take enforcement actions based on information security shortcomings will require the target entity to implement and maintain such a program, and they will further require periodic audits by a third-party assessor for as long as 20 years. Implementing (and documenting) a program of this nature can mitigate the risk of a security breach, improve the protections you provide to customers' and employees' data, and help demonstrate to inquiring regulators that any security incident you do experience did not result from negligence.

Q Do you know whose information you are maintaining?

Your organization probably maintains personal information about current and former employees. It also may hold information on job applicants, business partners, customers, and consumers. To know your privacy compliance obligations, you need to understand your relationship to these individuals (that context sometimes reveals a compliance requirement with respect to a subject-matter-specific privacy law, such as the Fair Credit Reporting Act) and where they are from (since the state or country where they reside will seek to apply its privacy laws to your organization). Identifying these individuals will identify the primary legal requirements that your compliance program needs to address.

Q Are you prepared to respond to an information security breach?

As mentioned above, multiple sources of law dictate that your organization must notify affected individuals if personal information is breached. The steps to responding begin well before the notification is sent, however, and include investigating and mitigating the incident, identifying which laws apply (generally based on the individuals' residency), consulting insurance coverage, forming a response team within your organization, and developing a sense of your organization's exposure once the breach is public. Most laws require that notice be provided "without unreasonable delay," and some set a firm (and short) deadline of 45 or 60 days to provide notice. Therefore, preparing for a breach before it occurs is a crucial compliance step.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Does your compliance program include sound vendor management?

Privacy and information security laws hold "data owners" responsible for the acts and omissions of their service providers with respect to the personal information those providers access. Those responsibilities include notifying affected individuals of a breach that occurred regarding data maintained by the provider on your organization's behalf (and providers are the cause of a breach 44% of the time). Some of the state laws alluded to above affirmatively require diligence and contractual provisions where providers will handle personal information. In short, providers are a big source of risk, whether they handle data recovery, provide data hosting, manage hard copy records for storage, process payroll records, or provide employee benefits. If they handle personal information, your program should provide a systematic process for vetting their privacy and security practices and for the consistent inclusion of appropriate contractual protections.

Is your health plan up to date with new HIPAA requirements?

Thought your health plan's HIPAA implementation was long-since complete? Last year the economic stimulus bill included substantial changes to the obligations of HIPAA-covered entities (including group health plans) and their service providers (business associates). New policies, procedures, and training are all required, and existing contracts with business associates will require revision. As above, there is a new breach notification requirement, so your plan will need to be prepared to notify individuals and the Department of Health and Human Services. Providing those notifications raises the stakes on the need to demonstrate that your plan was fully HIPAA-compliant at the time of the incident. In addition, HIPAA penalties recently increased from a per requirement annual maximum of $250,000 to $1.5 million, and state attorneys general have recently-earned the right to enforce these requirements.

Does your organization train employees on privacy and information security?

Where privacy and information security are concerned, your employees are both your greatest risk and your first line of defense against compliance problems and security breaches. Well-meaning but untrained employees are a source of security breaches through any number of scenarios, such as losing portable devices storing personal information, leaving paperwork containing personal information in a car that is subsequently stolen, exposing personal information inadvertently through use of peer-to-peer file-sharing programs, or inadvertently sending personal information to an incorrect recipient. These same employees may engage providers without ensuring that information security is part of the diligence and contracting process, download a virus, start a new marketing program that inadvertently violates privacy-related marketing regulations, or engage in social networking activities that promote your company but unintentionally breach FTC guidelines on endorsements. By contrast, properly trained employees understand and appreciate the need to secure personal information and are your best defense against a security incident. Properly trained, your employees will engage in sound information security practices to mitigate the risk of a breach; they may be able to detect and prevent a breach; and if a breach occurs regardless, they will know to report it promptly.

In short, a comprehensive information security program is only as good as the employees implementing it. Regulators understand this principle, and demonstrating that training is available and conducted regularly will be a critical (and expected) part of demonstrating an effective information security program.

Does your organization regularly assess the effectiveness of its privacy and information security compliance program? If not regularly, are these assessments done in response to changes in the law or your operating environment? In response to a security incident?

To be fair, those were three questions rolled into one, but if the answer to any of them is "no," your compliance program may not be sufficiently up to date. Laws in this area are evolving rapidly, but even those changes become a blur if you focus on the speed with which our environment changes. Changes in technology and the increasing creativity of bad actors who would like to steal your data mean that your organization needs to reassess its program regularly. Once identified, gaps must be addressed, and the solutions (glancing back to the top of our list) must be fully implemented as part of your comprehensive information security program.

Just for the sake of discussion, let's assume you had some difficulty responding to some or all these questions. In that case, do not be discouraged. Compliance and risk management in privacy and information security can be achieved. The key is to work through the issues methodically, develop a work plan and budget based on priorities, and stick to it. Delaying will only exacerbate your compliance challenges since your organization is certain to collect and store more information, privacy laws will continue to proliferate, and associated risk will grow.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.