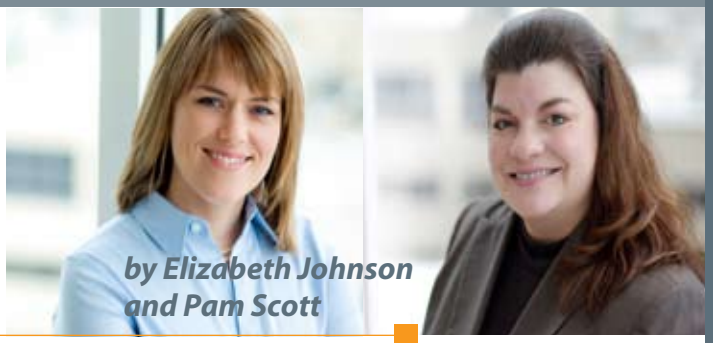
SEPTEMBER 2010

PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Do You Know Who's Got Your Data? It's Time to Pin Down Your Vendors and Make Sure They Toe the Line on Information Security



by Elizabeth Johnson and Pam Scott

Your organization may be minding its information privacy and security Ps and Qs, but are your vendors? From your payroll provider to your copy service, from your data hosting provider to your records disposal service, dozens of third parties handle personal information on your behalf, and your information security program is only as good as theirs.

Identifying these service providers and obligating them by contract to implement necessary security measures is mandatory in many states and thus necessary to comply with law. Forty-six state laws and several federal rules require your organization to notify affected individuals of any breach your providers may cause, making appropriate diligence and contracts necessary to avoid costly data breaches and related risks. The Ponemon Institute's 2009 study of data breach costs indicates that 42 percent of the breach incidents studied were caused by third-party mistakes, and the involvement of those third parties increased the cost of the breaches by 12 percent.

Examples of contractor missteps that have caused recent data breaches include:

- Tossing boxes filled with the personal information of tens of thousands of individuals into open dumpsters and recycling bins.
- Publishing login credentials in a brochure and on the Internet for a secure website that contained hundreds of thousands of individuals' personal information.
- Leaving an unencrypted laptop containing personal information of thousands of individuals in a car, from which it was stolen.
- Losing a shipment of computer backup files and unencrypted CDs containing personal information for tens of thousands of individuals.

In all cases, the organizations that hired these contractors were obligated to give notice of the breaches. These incidents typically result in bad press, government enforcement actions, lawsuits, and lost productivity while the organization responds to the breach. The average cost to respond? Over $6.5 million.

So how do you comply with information security laws and avoid cleaning up a contractor's costly data breach? The most effective solution is to implement a comprehensive privacy and security compliance program that includes vendor management. The first step to vendor management is to actually identify all the contractors that access your data. The next step is to conduct appropriate diligence on their security programs, which can consist of a questionnaire, a conversation, an onsite review – any level of checking is better than doing nothing.

Arguably the most crucial step in vendor management is executing a strong contract that is agreed to before the first piece of sensitive data reaches the contractor's hands. As above, a number of states require contracts by law when a service provider will have access to or dispose of personal information. Contractual issues to consider include control of subcontractors a service provider may use; compliance with applicable information privacy and security laws; appropriate security measures such as encryption and system activity review; notice and cooperation in situations involving data breaches; the right to audit the contractor's compliance and security program; and appropriate allocation of responsibility and liability in the event of a breach.

Our Privacy and Information Security Practice can help you develop an appropriate vendor management program, streamlining diligence efforts, addressing common contracting issues, and assisting you in negotiations.

Elizabeth Johnson may be reached at 919.783.2971 or ejohnson@poynerspruill.com. Pam Scott may be reached at 919.783.2954 or pscott@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW