Wiley Rein & Fielding LLP

Outsourcing, off-shoring and monitoring your vendors

By Kirk J. Nahra

The widespread growth in national, state and international privacy laws in the past few years have created enormous compliance challenges for most companies that deal with any kind of personal information – about employees, customers or others. The ongoing debate about expanding these laws creates consistent confusion and the need for a flexible approach to a difficult compliance challenge.

For many companies, control over vendors is a weak spot on privacy compliance (as well as in other areas of compliance – for example, note the recent case filed by the New York Attorney general against pharmacy benefit manager Express Scripts, which named CIGNA as a defendant in connection with its oversight of Express Scripts). Companies spend millions of dollars on their own internal compliance challenges, but then provide all the same information about individuals to vendors, who may be unregulated or unsophisticated about privacy concerns. The vendors may have far fewer concerns about customer relations – because the individuals are not their customers. And, in the current political climate, these vendors might be "off-shore," creating both regulatory concern and public apprehension. In addition, the "subcontracting stream" may mean that companies don't even know where their individual information is being sent. So, what are the main issues and what should be done?

The Regulatory Climate

With the increasing regulation of personal information, restricting the use of vendors is a common component of most new compliance requirements. The HIPAA Privacy Rule, for example, has created a cottage industry for the development of "business associate" contracts, where a HIPAA covered entity needs to enter into a business associate relationship with essentially any vendor who receives or utilizes protected health information from or for the covered entity. Read closely, the regulatory requirements mandate only specific contracts terms, including taking action when the covered entity knows that a business associate has breached the Privacy Rule, but there is no clear obligation to "monitor" these vendors. Covered entities across the country are now evaluating whether the HIPAA Security Rule, with its "close but not the same" business associate requirements, now creates an additional obligation to monitor vendors.

The Gramm-Leach-Bliley regime for financial institutions is similar. GLB, in its privacy requirements, dictates very little for vendors. In many instances, there were no contractual requirements at all. In other situations, the financial institution simply needed a contract that obligated the vendor to use the personal information received from the financial institution only for purposes of performing services for the financial institution. No "monitoring" was required.

The GLB security provisions created some modest additional monitoring obligations, with many companies still evaluating how best to monitor their vendors within the limited regulatory requirements.

Why Monitor?

So, under many privacy laws, there is not a formal compliance violation if a company fails to monitor the activities of their vendors. Does that mean companies should not monitor?

On the one hand, there are those who would argue that taking on a "voluntary" obligation to monitor takes on its own risks – by taking on a responsibility to monitor, the company creates an obligation to follow through on the monitoring, with risks if this oversight is not done effectively. Taking this position is not unreasonable, but, in the current environment, does not seem to be the right approach.

Why not? Let's focus on the few situations where problems have arisen. The most famous incident – which has generated publicity and responsive action far in excess of the magnitude of the specific event, involved a medical transcriptionist in Pakistan who, at the end of a series of subcontracting relationships, "threatened" a hospital with posting patient names and information on the Internet, unless the transcriptionist got better pay. This story was covered in newspapers around the country (and the world), all of it identifying the hospital in question (who apparently had no idea that its vendors had subcontracted to Pakistan), with enormous adverse publicity and a wide range of new legislation drafted to respond to this problem. So, adverse publicity and reputational damage is a real and significant concern – perhaps beyond the (so far) limited risks of privacy compliance enforcement by regulators. So, as this example and others have indicated, the most "realistic" risks are not compliance-related, but instead from other public problems and due diligence or overall risk management concerns.

Offshoring vs. outsourcing

One other factor to consider, before developing an appropriate risk management and compliance plan, is to distinguish between "outsourcing" and "off-shoring." Outsourcing involves hiring a vendor to perform a service on behalf of a company. "Off-shoring" typically is a subset of "outsourcing," and involves retaining a vendor who is based outside the Untied States (although companies also need to consider the risk implication of a limited range of "off-shoring" that is not "outsourcing" – where a company as a subsidiary or affiliate in another country that handles particular aspects of a company's business). Off-shoring creates numerous issues, some of which (for example, the interaction of various international privacy rules) are outside the scope of this analysis.

Off-shoring has lead to the largest outcry in the privacy area. First, the Pakistani story received increased attention because it involved off-shoring. A transcriptionist in Houston would not have generated the same kind of publicity. In addition, off-shoring also creates the perception (accurate or not) that the privacy rules cannot be enforced in other countries. Also, there are clear public relations implications where information is sent off-shore and somehow mis-used. Last, and perhaps most important, off-shore privacy issues have merged with the visible political question of whether off shore outsourcing costs Americans their jobs. This

combination of factors has lead to a variety of proposed legislation at both the state and federal level that prohibits or restricts off-shoring. One proposed law, in California, would have required permission of individual customers before their information could be sent to an off-shore vendor.

Latest Developments

So, what is happening on this front? There have been a couple of important developments that are increasing the pressure on outsourcing and off-shoring.

- In June 2004, the Federal Deposit Insurance Corporation issued a publication entitled "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks." This study "presents the FDIC's findings with regard to the associated risks of offshore outsourcing by financial institutions from a safety and soundness perspective and with a particular emphasis on the threats posed to customer privacy." While focused on financial institutions, this study (located at http://www.fdic.gov/regulations/examinations/offshore/index.html) is a must-read for any company considering off-shore outsourcing.

- A professional organization of certified public accountants, the American Institute of Certified Public Accountants, also has issued proposed new ethics standards covering the outsourcing of professional work to third parties. Under these standards,

  - a member would be required to inform clients of the use of a third party service provider before sharing confidential client information with that provider;

  - a member using a third-party provider would be responsible for all work performed by the provider; and

  - a member using a third-party provider should enter into a contractual agreement with that provider to ensure the confidentiality of client records.

While still in a proposed form, the AICPA has indicated that while the controversy that led to the new proposal primarily related to offshoring, the "guidance concerning the use of third-party service providers should apply equally to service providers located domestically and abroad." This proposed rule is located at http://www.aicpa.org/index.htm.

- In addition, in a recent presentation to the American Bar Association, an "operations risk specialist" for the Federal Reserve Bank of Atlanta indicated that off-shoring relationships were going to become an increasing part of review and oversight of financial institutions. This official indicated that any bank weighing offshore contracting should make its decision only after a "slow and methodical analysis," saying such moves carry significant risk and variables. In addition, he indicated that regulators expect financial institutions to put in place a number of safeguards, such as ongoing monitoring of offshoring arrangements by staffers with a particular expertise in monitoring these arrangements.

Best practices?

So, with all of these developments and constant pressure on additional laws and regulations (one report identified at least 186 pieces of legislation at the federal and state level dealing with off-shore outsourcing), what is a company to do?

- Identify Your Goals: Compliance issues should be a high priority for any company. Where a law restricts outsourcing, or imposes monitoring obligations, these laws should be followed. However, compliance should be a minimum standard, not a maximum one. Companies should aggressively review the other risks from inappropriate outsourcing which, in many contexts, might be more substantial. At the top of this list are reputational risk and the risk of lawsuits by customers whose information has been used inappropriately off-shore.

- Identification of Subcontracting Arrangements: Companies should know where their information is being sent, particularly when it is being sent off-shore. This can be accomplished by a prohibition on subcontracting or an identification and approval of subcontracting relationships.

- Developing a Strategy for Monitoring Vendors: Companies must have a strategy for monitoring and overseeing vendors. This should include both a front end "due diligence" review, as well as ongoing oversight of the vendor relationships. For many privacy officials, this seems like a substantial challenge – and many privacy offices, especially those facing enormous contracting obligations such as with HIPAA business associates, have chosen a path of least resistance due to the volume of contracting requirements. For many companies, however, these kinds of arrangements may already be in place, just not within the privacy office. Many companies have due diligence questionnaires or other questionnaires as part of the initial contracting process. Many IT departments use similar risk management assessments to evaluate technology vendors. So, for many companies, this may be an easier process to start than it seems initially.

- Evaluation does not have to be one size fits all: Volume also creates other challenges – simply, an intuitive feeling in many companies that they can't possibly keep track of all the vendors. Accordingly, it is fair to base a vendor monitoring strategy on a realistic distinction between categories of vendors. For example, it makes sense to focus efforts on those vendors who use or disclose "critical" or particularly sensitive data. Similarly, the largest vendors – dealing with the most substantial volume of personal data, are "higher risk" than other vendors. Those vendors that have "client facing" responsibilities also should be in the high risk category. Beyond this, companies should be encouraged to develop a strategy that can concentrate oversight efforts on those vendors where there is the highest risk. For other companies, overall privacy risk can be managed through representations, provision of policies and procedures or other low effort means. Similarly, imposing prohibitions on subcontracting may reduce the overall universe of privacy concern for vendors.

- Jurisdictional Issues: One area that has crated substantial concern in the off-shoring arena involves whether privacy obligations can be enforced in foreign countries. Companies, to the extent they permit offshoring, should evaluate how best they can enforce contractual obligations – through choice of law provisions, agreements on jurisdiction, bonding requirements or otherwise.

- Mitigation Issues: Last, companies need to pay particular attention to how they will interact with vendors in situations where there has been a breach of a privacy or security obligation. AN increasing number of state laws (led by California's recent security breach laws) require specific actions in the event of a security breach. Companies need to have an approach to how they will manage vendors who are responsible for a confidentiality failure. Typically, vendors should agree to take all reasonable action dictated by the company. In order to make this provision meaningful, vendors must be required to report security or privacy incidents promptly and in specific detail, and the contracting companies must have an effective approach to managing these breaches, whether the responsibility is with the company or a vendor.

Vendor management remains an area of continued confusion and changing legal circumstances. Also, because of the volume of vendor relationships, this is an area where a significant use of resources may be necessary. However, as the wide range of pending legislation and broad publicity surrounding vendor incidents demonstrates, developing an appropriate program for managing vendor relationships is a critical component of an effective risk management program in the privacy and security area.

For questions or further information on off-shoring, outsourcing or other vendor issues, please contact Kirk J. Nahra at 202.719.7335 or knahra@wrf.com.