Managing data security and privacy risk of third-party vendors

The use of third-party vendors for key business functions is here to stay. Routine sharing of critical information assets, including protected health information (PHI), with cloud providers, consultants, business process outsourcers, third-party transaction processors, and other business associates has become standard business practice. Yet, inevitably, as data moves out of the organization’s protected infrastructure into that of a third-party vendor, a certain degree of control is relinquished. Organizations must remain vigilant and engaged in assessing risks to their data, even though it resides at a vendor location.

The negative publicity that health care providers, health plans and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) can encounter when having to post a data breach on the U.S. Department of Health and Human Services website is painful enough, but the potential impact of a lawsuit brought under the Health Information Technology for Economic and Clinical Health (HITECH) Act can be devastating. In spite of that, a number of breaches of PHI are occurring daily, and many are caused by third-party vendors.

Health care providers can’t afford to wait for federal regulators to perform audits on business associates, but must be proactive in protecting their information assets. How can they do so when entrusting them to third parties? Moreover, how can they ensure compliance with a changing landscape of security and privacy regulations?

At issue is the fact that many third-party vendors, which store, process or transmit personally identifiable information (PII), electronic PHI (ePHI) and intellectual property (IP) on behalf of users, may not have appropriate controls in place to secure the data, manage risk, or enable users to meet their privacy and security obligations. Even when an organization outsources data management and processing activities, regulations often require that it retain responsibility for ensuring that its data is protected.

The onus is on organizations to select vendors with a robust approach to risk management. In order to do so, they need to carefully vet vendors prior to selection and then actively monitor their security and privacy control environments throughout the life of the contract. Monitoring third-party data security and privacy risk requires a strong and effective process for ongoing vendor management that starts long before the contract is even signed.
Managing data security and privacy risk of third-party vendors

What is at risk?
Data breaches resulting from the use of third-party vendors are growing and have become exceedingly expensive to manage. In fact, according to a recent study by the Ponemon Institute, 39 percent of data breaches in 2010 involved third-party organizations such as outsourcers, contractors, consultants and business partners.¹ In a study conducted in 2011, the percentage of health care data breaches caused by third-party vendors was 46 percent.²

These breaches tend to be very expensive to resolve. For instance, the average organizational cost of a data breach in 2010 increased to $7.2 million, up 7 percent from $6.8 million in 2009. Total breach costs have grown every year since 2006. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from 2009.³ In the event of a breach, companies may also face fines, civil penalties and legal repercussions. Numerous lawsuits have been filed against health care providers that breach PHI. Some lawsuits seek damages that run into the millions.

For academic medical centers, theft of research IP is another growing threat, with global losses estimated to be in the billions of dollars. According to the FBI, the rise of digital technologies and internet file-sharing networks provides the means by which trade secrets, proprietary products, plans and schematics may be stolen. Much of the theft takes place outside of the United States, where privacy laws may be lax and more difficult to enforce.

Security and compliance
In addition to HIPAA HITECH, most health care organizations must comply with rules and regulations that address the handling of information assets, such as the Payment Card Industry (PCI) Data Security Standard (DSS) requirements, Clinical Laboratory Improvement Amendments (CLIA) and others. Many of these rules and regulations apply not only to user organizations that collect the information, but increasingly to third-party vendors that provide outsourced services.

There may be other rules and regulations to consider, depending on where your organization does business. For example, a growing number of states (e.g., Massachusetts, California, Texas, Michigan) now have their own privacy and security laws, and many other states are considering them. European Union countries, along with other international governments, also have specific data privacy and security laws.

Interestingly, a Ponemon Institute study revealed a difference in view between cloud providers and users about who is primarily responsible for security in the cloud.⁴ Nearly seven in 10 (69%) third-party vendors saw users of their cloud service as being primarily responsible for their own data security, while only 35 percent of users perceived themselves to be mostly responsible.

This apparent confusion about who is responsible for data security may lead users to become complacent about securing their data, since they may assume that their third-party vendor has strong security and privacy controls in place, when, in fact, that vendor may not. Simply put, users need to take a more proactive approach toward ensuring that their data is adequately protected.

¹ Ponemon Institute, LLC. 2010 Annual Study: U.S. Cost of a Data Breach (March 2011).
² Ponemon Institute, LLC. 2011 Second Annual Benchmark Study on Patient Privacy & Data Security (December 2011).
³ Ponemon Institute, LLC. 2010 Annual Study: U.S. Cost of a Data Breach (March 2011).
⁴ Ponemon Institute, LLC. Security of Cloud Computing Providers Study (April 2011).
**Managing data security and privacy risk of third-party vendors**

**What can you do to protect yourself?**

Organizations that are considering the use of third-party services need to perform appropriate due diligence when selecting and managing their relationships with vendors. Data security, privacy and compliance considerations should be top of mind.

During the due diligence process, organizations should ask a number of key questions about data security and privacy considerations:

**Data protection**
- How will data be protected?
- What controls does the vendor have in place for intrusion detection, perimeter security, physical security, timely application of security patches, and data leak prevention, among other safety measures?

**Data access**
- Who will have access to our data, and how can we confirm this?
- Does the vendor have the right security controls to protect our data? How will the provider ensure that others (e.g., those whose data resides on the same server as ours) are not able to view our data?

**Data security**
- What policies and procedures are in place to detect, prevent and mitigate incidences of identity theft?
- Have there been any instances of identity theft experienced by the third-party vendor within the last two years?
- Does the vendor scan employee email and company social media platforms for potential breaches of customer data?
- How are incidents and breaches reported?
- Will we receive notification if a breach to our data occurs?

**Disaster recovery and business continuity planning**
- Does the third party have a disaster recovery plan?
- In the event of a disaster, how will the vendor protect our information assets?
- Can we get our data back if the vendor goes out of business?

**Contract and controls compliance verification**
- Does the potential vendor allow third-party verification or provide such verification on its own?

Attestation reports — if vendors have them — can offer a useful perspective on a vendor’s security and privacy control environment. The AICPA’s Service Organization ControlSM (SOC) reports — specifically its SOC 2SM and SOC 3SM reports — provide service auditors and service organizations with reporting options that address controls related to security, availability, processing integrity, confidentiality and privacy. These reports help vendors demonstrate the strength of their controls to current and would-be customers; however, it is up to prospective users to evaluate these reports with care. Users must carefully read and thoroughly understand their content, evaluate any findings in the context of the outsourcer’s services that they are considering, and determine how weaknesses in their own user control environment may affect the overall control environment.

During the due diligence process, organizations should ask a number of key questions about data security and privacy considerations.
Establishing an effective vendor management program

If your organization does not currently have a vendor management process, putting one in place can seem insurmountable. We generally recommend that our clients approach vendor management as a three-stage process: first, identify and implement “quick wins”; second, establish a standardized, streamlined vendor management process; and third, enhance the vendor management process with ongoing attention to vendor risk management.

1. **Identify and implement quick wins.**
For many companies, a vendor inventory either does not exist or is out-of-date. Business associate agreements (BAAs) or service level agreements, likewise, may not be kept up-to-date. As a result, the first step is to identify the vendor population by determining which vendors have access to confidential or sensitive data and how much PII/ePHI is collected, used or disclosed by those vendors.

   If a SOC 2 or SOC 3 report is not available, conduct a quick privacy and security risk assessment against the inventoried vendors by using surveys, questionnaires or on-site visits. Questionnaires should inquire about a range of controls related to financial stability, adoption and enforcement of robust security and privacy controls, performance, and other crucial topics. Identify the control gaps and risk-rank gaps for each vendor. Based on these risk assessment results, flag high-risk vendors.

   Once high-risk vendors have been identified, focus on getting them to mitigate the most immediate risks by implementing data protection solutions, digital rights management, or other actions to minimize data security and compliance risks.

2. **Develop a streamlined vendor management process.**
Going forward, it is a good idea to develop and implement a standard process for assessing and monitoring changes to vendors’ data security and privacy risk environments, in addition to looking at the traditional set of vendor management criteria such as financial stability, ethics, manufacturing/service quality, order fulfillment and invoice accuracy. The results of vendor questionnaires, on-site inspections and attestations may be compared from year to year, in order to identify potential degradation in the security control environment.

3. **Establish an ongoing vendor risk management approach.**
When outsourcing or co-sourcing high-risk business functions, such as processing health claims or tracking account transactions, consider establishing strategic vendor relationships, as well as adopting a centralized approach to managing the vendor population and associated risks. Often internal audit takes the responsibility for managing and evaluating vendor risks.

   Through this process, many organizations can pare down the number of vendors to which they entrust their information assets. In so doing, organizations may be able to reduce the vendor risk and at the same time, take advantage of special discounts to decrease vendor costs.
Develop ongoing processes for evaluation and monitoring
Ultimately, health care providers should put in place a consistent process to assess, monitor and manage risks related to vendor operations. (See “Establishing an effective vendor management program” on the previous page.)

Even though many organizations execute vendor agreements with service providers, too few of them build protections into the contract to support an ongoing program to monitor and assess vendor control risks. For example, organizations may insist on a right-to-audit provision that gives them the authority to periodically audit and monitor controls on-site, whether or not a SOC 2 or SOC 3 reporting process is in place. If the vendor is not willing to allow the provision — particularly if a SOC report or similar attestation report is not available — the user organization may wish to reconsider its options.

Looking ahead
The use of third-party vendors for key business functions has become standard business practice, but the security control environments of vendors vary greatly. It is essential for organizations to be vigilant in assessing risks to their data, even when they reside at a vendor location.

History shows that vendor data breaches may result in fines, civil penalties and loss of the public’s trust. In the event of a data breach, anticipated cost efficiencies and other benefits can evaporate as a result of costly breaches and enforcement actions. Intellectual property may be similarly at risk, which can cost the organization dearly in terms of lost investment and reputation.

Health care providers considering the use of third-party vendors need to ask themselves, “Once we share our information assets with third-party vendors, will we still be in compliance?” Those that wish to answer affirmatively must be prepared to spend time vetting their vendors and carefully monitoring their security and privacy control environments over time.

For more information
Jan Hertzberg
Managing Director
Business Advisory Services
jan.hertzberg@us.gt.com

About Grant Thornton
The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the six global audit, tax and advisory organizations. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

Content in this publication is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information on the issues discussed, consult a Grant Thornton client service partner.

www.GrantThornton.com
© Grant Thornton LLP
All rights reserved
U.S. member firm of Grant Thornton International Ltd