Third-party relationships and your confidential data
Assessing risk and management oversight processes
As the volume of electronic medical data has grown, so has the number of third-party custodians that handle it. Organizations increasingly rely on third parties for infrastructure, managed applications and data management. Navigating the changing rules governing these third parties has become more complex. Organizations now face the additional responsibilities and challenges of user access management, change management and data stewardship, even though they don’t own the structure or directly manage the resources involved. The risk of these relationships is significant: third parties have been responsible for almost half of all data breaches.

Compounding these challenges are new federal requirements and continuously evolving state requirements for managing electronic protected health information (ePHI). Important changes that take effect Sept. 23, 2013, in the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule broaden the definition of a business associate, set new limits on how data may be used, redefine what constitutes a breach and establish new civil penalties for violations.

The changes underscore the need for companies to carefully select third-party vendors using risk-based criteria. Failing to properly assess risks inherent in these relationships and failing to implement effective monitoring controls can be costly in terms of potential penalties and damage to an organization’s reputation.

The challenge for internal auditors at health care providers relying on third parties is determining if vendors hired to store, process or transmit electronic protected health information have the processes and controls in place to secure data, sufficiently manage risk, and meet privacy and security requirements. Internal audit can now play a key role by testing management’s risk assessments and due diligence activities in selecting vendors, and by reviewing the functionality of management’s oversight role of this process.

**HIPAA Act: What’s changed?**

- Broader definition of business associate
- New limits on the use of information for marketing and fundraising
- Tiered civil penalty structure
- “Breach” is redefined and now requires a breach risk assessment
- Four-tiered risk assessment replaces the harm threshold in identifying a breach

Source: Grant Thornton LLP
The growing demand for data custodians
The volume of electronic medical data is growing rapidly, driven by the potential quality of care considerations, desired process efficiencies, cost savings and looming federal requirements to migrate all health care providers to electronic records by 2015. In the past year, the use of electronic medical records has more than doubled, and the U.S. Department of Health and Human Services (HHS) has already exceeded its goal to have 50% of doctors’ offices and 80% of eligible hospitals using electronic records by the end of 2013. It would be almost impossible, not to mention cost-prohibitive, for health care providers to manage this explosion of electronic medical data on their own. This tight timeline and increased demands on organizations to manage the necessary technologies and infrastructure have resulted in an increase in the number of third-party custodians that handle the data.

The Omnibus Rule changes in HIPAA increase the responsibility on health care organizations to select third-party vendors with strong risk management and compliance procedures. No one wants to face the expense, not to mention the public backlash, from a data breach.

Health care auditors and compliance specialists can play a key role by assisting management in their responsibilities to identify compliance risks and establish effective vendor monitoring as the use of third parties becomes more prevalent.

The types of third-party relationships
Companies hire outside firms to manage information technology (IT) in one of three ways:

- **Infrastructure only.** A third party provides key infrastructure, such as a network and servers, and their administration but doesn’t provide any applications or application support (e.g., third-party data centers)
- **Managed applications.** The third-party provider exerts some control over installation, maintenance and support of the infrastructure and applications
  Managed applications — including cloud computing, infrastructure and software-as-a-service — can be used to more rapidly deploy software to a larger number of users across a network, and reduce the capital needed to support and manage applications over an extended period of time
- **All data.** Includes infrastructure and managed applications, as well as support, maintenance and disaster recovery aspects of the infrastructure and applications (e.g., backup and recovery site)

---

These third-party relationships offer a host of benefits for health care providers. Contracting with an outside firm to manage data systems enables providers to streamline their IT systems and related processes, and accelerate the deployment of IT resources, such as new software. These relationships also allow health care providers to focus key limited people resources on vision and mission critical activities.

However, third-party relationships also present new risks. Simply using another company’s infrastructure or services doesn’t always reduce potential vulnerabilities that could compromise ePHI. Relying on third-party vendors means allowing data for which your organization is responsible to move outside your chain of custody. Once a health care organization enters into a third-party relationship, it faces the challenge of compliance requirements for computer networks and software that another company owns. What’s more, the organization is dependent on such third parties for the reliability and availability of mission-critical data systems, which may include applications that require instant and constant availability (e.g., clinical applications).

For health care providers, the stakes are huge. The potential for a data breach poses tremendous compliance, reputational, and financial risks. Third-party custodians — outsourcers, contractors, consultants and business partners — accounted for more than 33% of all breaches in 2010 and 46% in 2011. Companies whose data is compromised may suffer damage to their reputations due to the negative publicity resulting from the required disclosures under the Health Information Technology for Economic and Clinical Health (HITECH) Act. Such disclosures include having information related to any breach affecting 500 patients or more publically available on the HHS website, which can trigger adverse media coverage and class-action suits. Potential damages in such litigation can run into the millions of dollars.

Even without legal action, data breaches can be expensive. Average organizational privacy breach-related remediation costs have grown every year since 2006 and by 2010 had topped $7.2 million.

---

2 “Managing data security and privacy risk of third-party vendors,” Grant Thornton CorporateGovernor, Volume 2, Fall 2011.
3 Ibid.
In January 2013, HHS published the HIPAA Omnibus Rule (Final Rule), which includes a comprehensive privacy and security risk assessment as a component of HIPAA compliance. The new rules, which providers must comply with by Sept. 23, 2013, expand the definition of a “business associate” to include anyone who maintains protected health information in either electronic or paper form and set new limits on using ePHI for marketing and fundraising purposes. Covered entities and their business associates are prohibited from selling patient information without the patient’s permission.

The new rules also create a tiered penalty structure for violation of the HITECH Act, with the fines escalating in conjunction with the severity of the violation. In addition, improper use or disclosure of protected information, including ePHI, will be considered a breach unless the provider or the custodian can show a low probability that data was compromised.

Proving this will no longer be simply weighing the risk of potential harm to the patient. Now, providers and third-party custodians must consider four factors in determining if a breach occurred:

- Could the patient be identified by the data?
- Who received or used the information and to whom were the disclosures made?
- Was the data actually acquired or viewed by someone who should not have had access to it?
- What steps were taken to mitigate the risk? Has the recipient of the data given assurances that it was not used inappropriately?

The new rules put a greater onus on providers and their auditors to understand all aspects of third-party ePHI risk and develop a process for minimizing it.

Assessing third-party risk
Management must set the tone for a culture of compliance, both internally and with third-party vendors, and frequently reinforce the importance of ongoing risk management with employees and business associates. Internal auditors can add value to management oversight of vendors by assuring compliance practices are followed by custodians of an organization’s ePHI. This would be accomplished through an appropriate combination of inquiry, site visits, periodic meetings, testing, and review of third-party privacy and security practices.

Before auditors can assess the risks associated with a vendor’s processes, they must first understand how data resides and moves within their own organizations — who handles information and what technologies are used in collecting, transmitting, storing and moving data from in-house systems to third parties. This level of understanding will also help identify potential deficiencies in vendors’ systems. Understanding the work flows at the data level provides auditors with a twofold benefit:

**HITECH Act notification rules for data breaches**

Following a breach, covered entities and their business associates must notify the following:

- HHS is reported to annually via a website for breaches affecting fewer than 500 individuals
- HHS and the media are notified within 60 days of determination that a breach affects 500 or more individuals and meets the Federal Breach Reporting Requirements
- Patient notification is required under both federal and state laws with varying notification requirements

Source: HHS

**Notes:**

first, they will be able to understand the location of ePHI and have a comprehensive inventory of the most critical applications; and second, as work flows change and technologies are replaced with new applications, they will be able to more quickly understand the impact of those changes on the high-risk work flows and whether or not the changes have implications for patients and the organization.

For example, consider the difficulty in assessing the risk posed by the proliferation of mobile devices. Keeping an accurate inventory of the devices, encryption status and potential information breaches is already challenging. Some organizations have resisted encryption because it slows down devices. Similar concerns extend to third-party vendors, as well. Auditors must also determine if a vendor’s employees or subcontractors have access to a health organization’s ePHI via mobile devices and how those risks are monitored. Many data breaches have occurred because an unencrypted, lost or stolen vendor laptop contained critical or proprietary data.

After reviewing the vendor inventory to determine what data third parties collect, store and transmit, the next step is to confirm where the data resides within the vendor’s system. Do they store it on their own servers? Do they use a cloud service? Do they transmit the data using proper encryption? Vendor management begins before the contract is signed. Contractor agreements should be developed to specify how ePHI will be protected once it leaves a provider’s network and what the third party will do to ensure compliance. These agreements should include:

- policies for document storage and disposal;
- data management processes, including methods for tracking and controlling records — such as dates and time stamps — as well as the type of data sent and received, and the individuals who have access to records;
- descriptions of the vendor’s privacy and security programs;
- descriptions of output reporting — either electronically or in hard copy — so data can be reviewed, monitored and reconciled;
- periodic staff training in secure records handling and providing, and appropriate document management tools;
- staff responsibilities for ensuring compliance and allocation of sufficient job time to the task;
- right-to-audit clauses; and
- communication requirements regarding control deficiencies identified through internal or external sources.

Contractor agreements should be developed to specify how ePHI will be protected once it leaves a provider’s network and what the third party will do to ensure compliance.
Vendor selection and management
Organizations should establish a management process for properly vetting vendors before their selection, and then actively monitor vendor security and privacy controls to reduce the risks created by third-party relationships. To be effective, the overall process will require more formality and rigor in vendor management than in the past.

Establishing effective controls within a vendor management program requires a few basic though not necessarily easy to achieve steps:

1. **Identify your vendor population.** At many organizations, complete vendor inventories either don’t exist or are out of date. Before you can audit vendors’ compliance, you first must know who they are. This list should include any smaller third-party contracts that may have been added at the department level rather than through the typical centralized review and centralized contracting channels. These smaller arrangements may actually hold some of the higher risks because the contracts may not be as complete, and smaller vendors are less inclined to have the level of controls found with larger organizations.

2. **Develop a risk profile of all vendors.** Once you have completed the custodian inventory, establish risk criteria and conduct a privacy and risk assessment using questionnaires, surveys and on-site visits. Focus the inquiries on vendors’ controls and financial stability. Ideally, this type of risk profile should be developed by management for auditor review, but it may require the auditor to lead and/or complete the effort. If completed by the auditor, the auditor should work with management on developing a process to maintain it on some periodic basis, as discussed more below.

3. **Focus on highest-risk vendors first.** After the high-risk vendors have been identified, work with management and the vendor to mitigate the most immediate threats, using concepts such as data protection and digital rights management to close risk gaps.

4. **New vendor screening.** Develop a comprehensive process for selecting and monitoring new vendors. Once you’ve identified key vendors in your existing inventory, don’t allow the information to lapse. Create standard criteria such as ethics, financial stability, good references, invoice accuracy and service quality to assess new vendors and their technologies for protecting data. In decentralized environments or environments where departments can create vendor relationships without a central conduit such as purchasing or legal, ensuring this happens will be much more difficult and will require more internal audit consideration and efforts.

5. **Establish ongoing monitoring processes.** Continue to use surveys, questionnaires and inspections to review the compliance of third parties on an ongoing basis. Year-to-year comparisons can flag potential lapses in security control environments.

By centralizing vendor selection and oversight management and inclusion of an internal audit role, an organization can focus on reviewing the highest risk functions such as processing health claims and tracking account transactions. Consolidating third-party services can help management pare down third-party inventory, reduce the risk exposure and strengthen relationships with remaining vendors, which may generate discounts that reduce vendor costs.
Create standard criteria such as ethics, financial stability, good references, invoice accuracy and service quality to assess new vendors and their technologies for protecting data.

These benefits also come with certain risks. Storing ePHI on a cloud outside a health organization’s control is one. Transmitting data via the Internet or a wireless network is another. Perhaps the most difficult risk to assess, though, comes from third-party vendors that themselves subcontract with another cloud service provider, and the nature of those relationships. The result is a multilayered risk profile that presents complex issues for auditors. Each of these layers must be evaluated for further risk identification.

From an internal and IT security audit perspective, cloud computing risks can be divided into six areas:

1. **Data security and controls.** As with other third-party custodians, providers must assess the strength of a cloud vendor’s internal controls to protect the confidentiality, integrity and availability of ePHI.

2. **Data transmission.** Controls relate not just to hardware, but also to transmission. Data may be transmitted via the Internet or wireless networks. Is there adequate encryption? In selecting cloud computing vendors, providers must ensure they comply with all legal requirements, foreign business standards and specific regulations for the country or state in which the data is transmitted and stored. Is there a defined service level agreement for data transmission, and does your organization have the correct tools in place to assess compliance?

3. **Multitenancy.** This requires health care organizations to consider the possible comingling of data on shared hardware. Auditors should determine if data is properly segregated on the cloud and if the cloud operator has adequate controls to protect data both in storage and during transmission.

4. **Location.** Moving data to the cloud means moving assets to a remote location that the health care provider doesn’t control. Auditors should be aware of all locations maintained or contracted for by the cloud operator and guard against the risk a cloud operator could unilaterally move the data to another location without first informing the health care organization.

---

**Cloud computing**

Cloud computing is one of the emerging and rapidly growing challenges to the integrity of ePHI. Cloud computing provides access to a variety of information resources — software, development tools and remote access to infrastructure such as desktop computers and servers. The cloud, in most cases, is a server network and software managed by a third party in either a private or shared environment.

In health care, cloud computing can support electronic medical records, prescription data, practice management, computerized physician order entry, billing and administration. Clouds offer flexibility and affordability, enabling providers to expand resources as their needs dictate while paying only for what they use. Cloud computing reduces the need for capital investment in IT infrastructure and speeds the deployment of new applications and software updates. As a result, cloud computing use is rapidly growing within the health care sector.
5. **Reliability.** When relying on a shared resource such as the cloud, health care organizations face the risk that resources may not be available when they’re needed. Auditors should assess a cloud company’s ability to scale its systems to meet short-term surges in demand, as well as long-term growth. They also should determine when the cloud operator typically conducts system maintenance and installs upgrades to ensure data is available during peak business hours.

6. **Sustainability.** Auditors should determine the adequacy of a cloud provider’s disaster recovery and business continuity plans to understand how operations will continue if the cloud is out of service. Auditors may want to conduct a service disruption test to monitor the effectiveness of a cloud vendor’s response. Health care organizations should also have a plan for moving data if the cloud provider goes out of business or for when the contract ends. They should also assess the risk of the cloud provider being unwilling or unable to return data.

---

**Key questions**

Health care organizations considering risks associated with third-party custodians entrusted with ePHI should first understand the implications of the Final Rule and any related state regulations, and then complete a robust risk assessment of its existing vendor relationships. A similar level of management due diligence is important before entering any contractual relationship with new vendors. Internal auditors can play a key role in such due diligence by asking management to ensure it understands if the vendor has the proper security controls in place to protect organizational data by, at a minimum, addressing the following key questions:

1. Who will have access to our data, and how can we confirm this?
2. Does the vendor have the proper security controls to protect our data?
3. How will the vendor ensure that its other clients — for example, other companies whose data resides on the same server — won’t have access to our information?
4. What subcontract or affiliation arrangements does the vendor have that involve our information? And what assurances is the vendor providing in this regard?
5. How will data be transmitted between the vendor and the organization, and for what part of the transmission process are the vendor and our organization responsible/at risk?
6. What controls does the vendor have for intrusion detection, physical security, data leakage prevention, timely application of security patches and other safety measures?
7. Does the vendor allow third-party verification of controls compliance, or does it provide verification on its own?
8. Does the vendor have a disaster recovery plan, and if yes, when was it last tested? Can the vendor provide the latest results and any related remediation plan?
9. In the event of a disaster, how will the vendor protect our information assets?
10. Can we get our data back if the vendor goes out of business or when the contract ends, and how much will it cost to get it back?
11. What policies does the vendor have to detect, prevent and mitigate incidences of identity theft?
12. Has the vendor had any incidences of identity theft within the past two years?
13. Does the vendor scan employee email and company social media platforms for potential breaches of customer data?
14. How are incidents and breaches reported?
15. How quickly will we receive notification if a breach to our data occurs?
16. How is the communication chain of command managed and monitored?
17. What are the plans for reviewing procedures and notifying of any issues identified?
18. Does the vendor conduct internal auditing of its controls and safeguards? How often are audits conducted, and will the vendor provide the latest reports and any related remediation plans?
19. Does the vendor engage an external auditor to perform review procedures and issue an applicable Service Organization Control (SOC) or Statement on Standards for Attestation Engagements (SSAE) No. 16 report?
Health care organizations considering risks associated with third-party custodians entrusted with ePHI should first understand the implications of the Final Rule and any related state regulations, and then complete a robust risk assessment of its existing vendor relationships.

**Conclusion**

Increased use of third-party vendors for applications and data processing services is a business model that is likely to continue, especially as organizations find it necessary to focus limited resources on core organizational objectives and contract out support services. Unfortunately, many have learned the hard lesson that expected cost efficiencies and other benefits associated with third-party custodians of an organization’s confidential data can quickly be outweighed by data breaches that result in fines, civil penalties and damaged reputations. With even more demands under the Final Rule, organizations need to ensure an appropriate level of management oversight of their third-party affiliates, with internal audit supporting those efforts.

Internal audit can play a critical role in assuring that the risks are being recognized and managed appropriately.

---

**Grant Thornton project team**

David Reitzel  
Principal, National Leader, Health Care IT Advisory Services

Eric Wendler  
Business Development Director

Donna Wachman  
National Marketing Manager, Health Care

**AHIA white paper project team**

Mark Eddy, CPA  
HCA Healthcare

Michael Fabrizius, CPA  
Carolina HealthCare System

Linda McKee, CPA (Board Liaison)  
Sentara Healthcare

Glen Mueller, CPA (Chair)  
Scripps Health

Mark Ruppert, CPA  
Cedars-Sinai Health System

Debi Weatherford, CPA  
Piedmont Healthcare

**About AHIA**

Founded in 1981, the Association of Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is a provider of resources for internal audit and other risk positions. Explore our website (www.ahia.org) for more information. If not a member, please join our network.
About Grant Thornton LLP

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. In the United States, visit Grant Thornton LLP at www.GrantThornton.com.

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.

© 2013 Grant Thornton LLP  All rights reserved  U.S. member firm of Grant Thornton International Ltd.