Addressing Privacy, Security and Other Pressing Healthcare Concerns
By Susan Haseley and Matthew Jackson, Protiviti

Historically, the healthcare industry has been one of the most heavily regulated and scrutinized in the United States, and all signs indicate that more pressure is rapidly approaching. President Obama has made it clear that his administration will increase federal involvement in advancing the healthcare industry’s utilization of technology while strengthening the overall privacy and security of health information.

In the age of on-demand information, patients are becoming more informed and increasingly concerned about issues facing the industry. Understanding where to focus time and resources is the first step to meeting this challenge. This article discusses several relevant issues facing the industry today, including the implementation of the HITECH Act, PCI Data Security Standards, and Red Flags Rules.

The Health Information Technology for Economic and Clinical Health Act

Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA) on February 13, 2009. Division A, Title XIII (Health Information Technology) is anticipated to have the most significant impact on strengthening the requirements set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the utilization of electronic medical records. Division B, Title IV (Medicare and Medicaid Health Information Technology) is anticipated to have the largest financial impact on the healthcare industry as it addresses the refunds and penalties associated with implementing components of the ARRA. The combination of Titles IV and XIII are commonly referred to as the Health Information Technology for Economic and Clinical Health (HITECH) Act.

As a result of increasing HIPAA compliance concerns, audits of covered entities were to begin in 2008, but the Department of Health and Human Services (HHS) has published little regarding audit results or proposed audit checklists. However, the October 2008 Audit Report by the Office of Inspector General (OIG) of the Centers for Medicare and Medicaid Services (CMS) found “agreed to deficiencies” in the CMS process for auditing compliance by covered entities. Among other goals, the HITECH Act aims to improve enforcement and auditing of HIPAA compliance to address these concerns. While significant guidance is still forthcoming, organizations should be assessing the impact of changes stemming from the HITECH Act (e.g., increased scrutiny on business associates, notification requirements in the event of a breach, etc.) as well as evaluating the sufficiency of their HIPAA compliance programs. In doing so, the following should be considered:

- Determine if adequate programs are in place to support compliance and promote consistency across the organization.
- Determine if the assets that hold, store, process, and transmit electronic protected health information (ePHI) have been identified accurately. Asset inventory is a core component of the risk assessment process that is the foundation to a successful compliance.
• The inventory should include applications, databases, servers, online storage, and any other storage media that would hold ePHI.
• Ensure that unstructured data has been considered as well. The proliferation of ePHI commonly results from the use of Access databases and Excel spreadsheets for reporting purposes. Frequently these tools are loosely controlled.

Additionally, the ARRA includes funding provisions for investments in health infrastructure, personnel training on the use of health information technology (HIT), dissemination of best practices, and miscellaneous HIT adoption grants. While the funds appropriated to healthcare are not a high percentage relative to the ARRA’s total cost of $787 billion, they are still significant to healthcare organizations.

While stipend benefits are available in the near-term, long-term penalties will be instituted for non-compliance with the HITECH Act in the form of reimbursement reductions. The HITECH Act includes separate Medicare funding to provide physicians and hospitals with incentives for the adoption and maintenance of electronic health records (EHRs). Qualifying Medicare Advantage organizations are also provided incentives. Medicaid incentives are issued for physicians, other providers, and hospitals that meet the volume requirements for treating Medicaid patients. Eligible professionals include non-hospital based physicians, nurse mid-wives, nurse practitioners and certain physician assistants with at least 30 percent of patient volume ascribed to Medicaid patients, and pediatricians who are not hospital-based and have at least 20 percent Medicaid volume. As with Medicare, hospital-based physicians are not eligible for Medicaid incentives.

It is important to note that physicians and organizations are eligible to receive only one incentive regardless of whether they qualify for more than one. For example, in order to qualify for Medicaid payments, a provider must waive the right to Medicare incentives. Given these guidelines, it is critical for organizations to understand how and where they can obtain the most funding.

The Payment Card Industry Data Security Standard

Another area of increased focus for healthcare organizations is the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is a set of comprehensive requirements for enhancing payment account data security to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. All organizations joined together with the goal of enhancing payment account data security by driving education and awareness of security standards.

Many organizations, especially those in the healthcare industry, have been downplaying the PCI-DSS requirements since the card brands enforce them instead of regulatory agencies. However, heightened attention is being paid to these requirements, especially since last October’s release of version 1.2 of the PCI DSS. The changes resulting from this latest update are anticipated to shift the focus to many of the smaller merchants (which include many healthcare organizations) that, from a payment card perspective, have been operating under the radar for quite some time. However, the most significant change in the new version is related to the scoping of a PCI compliance effort. Historically, scoping was limited primarily to cardholder systems, defined as those storing, processing, and/or transmitting cardholder data. Version 1.2 makes it clear that if
cardholder systems share network segments with non-cardholder systems, then all systems could be considered in scope for PCI controls.

Organizations need to make a somewhat complex determination as to merchant level and applicable validation requirements while working closely with applicable acquiring banks. Numerous factors come into play, such as the number of discrete merchant IDs being used by a particular organization, the number of transactions conducted annually for any card type, what acquiring banks are being utilized, whether areas such as cafeterias and business offices are accounted for, etc. Depending upon any combination of these factors, acquiring banks or card brands may require validation via a self-assessment questionnaire (SAQ). The SAQ is simply a summary of PCI-DSS controls. The controls for each organization will vary based on the method(s) used to conduct credit card transactions. However, it is critical that gap-assessments and remediation strategies be based on the PCI-DSS and not a validation instrument such as the SAQ.

In general, however, all merchants are required to be in compliance with the 250-plus PCI-DSS controls. Organizations should assess the applicability of the PCI-DSS on a periodic basis and ensure appropriate mechanisms are in place to secure payment account data. Third-party companies authorized to validate an entity’s adherence to PCI DSS requirements are referred to as “Qualified Security Assessors” or “QSAs.” The quality, reliability, and consistency of a QSA’s work provides confidence that cardholder data is adequately protected. While a QSA can help assist in these efforts, it is important to note that a QSA quality assurance program starts soon and the work of QSAs will be put under the microscope. In other words, an independent party will verify their work, and undoubtedly will be more stringent going forward to ensure compliance with the standard.

The Federal Trade Commission’s Red Flags Rules

In November 2007, the Federal Trade Commission (FTC) and five federal bank regulatory agencies jointly issued the final rules and guidelines implementing sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act, commonly known as the “Red Flags Rules.” The FACT Act requires the development, implementation, and maintenance of a written identity theft prevention program by financial institutions and “creditors” for “covered accounts.” By definition, an organization is a creditor if it regularly:

- Extends, renews or continues credit;
- Arranges for someone else to extend, renew or continue credit; or
- Is the assignee of a creditor who is involved in the decision to extend, renew or continue credit.

Generally, healthcare providers are considered creditors if they bill consumers after services are completed. Setting up payment plans is a perfect example of where healthcare organizations extend such credit to patients. Healthcare providers that accept insurance are also considered creditors if the patient is ultimately responsible for the medical fees.

Additionally, a “covered account” is commonly an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions (e.g., credit card accounts, checking accounts, savings accounts, etc.). The Red Flags Rules clearly define what must be done by a creditor with covered accounts. Organizations should implement formal
written policies and procedures to address the following:

- The program must be created with the goal of identifying and incorporating red flags for covered accounts.
- Red flags that are included in the program must be detected.
- Red flags must be responded to appropriately (i.e., action must be taken).
- The program must be updated periodically to reflect the risk to the patient or to the safety of the creditor from identity theft.

Guidelines have been issued by the FTC, the federal banking agencies, and the National Credit Union Administration (NCUA) to assist with the design of an appropriate program. These entities also have issued guidance listing red flags that might arise in healthcare. Examples include:

- A complaint or question from a patient who received a bill for another individual
- Records showing medical treatment that is inconsistent with the physical examination or a medical history as reported by the patient
- A dispute of a bill by a patient claiming to be the victim of any type of identity theft
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance

Organizations should be working aggressively to implement their programs, as the compliance date has now been set as August 1, 2009 (based on a three-month delay issued on April 30, 2009). We recommend these organizations focus efforts on identifying additional red flags beyond the examples provided in guidance documentation. This guidance clearly states that it is not all-inclusive and is intended solely to be a starting point.

Application Implementation Practices

Meeting many of today’s challenges head-on requires the increased use of technology throughout the industry. Whether an organization is implementing a full electronic health records (EHR) system or merely upgrading a legacy system, there are many barriers that stand in the way of a successful implementation. In a recent survey portending just some of the challenges related to EHR, Gartner Group determined that 30 percent of all IT projects will never be implemented successfully. Furthermore, 51 percent exceed budget by more than 180 percent while at the same time delivering just 74 percent of the originally planned functionality.

Barriers to success may vary widely based upon the culture of an organization; however, it is not uncommon for any implementation to experience one or more of the following organizational issues:

- Lack of involvement/acceptance by physicians and employees
- Concerns about the inability to align workflow with a standardized EHR
- Concerns that automation of charting requires more time than paper charting
- Lack of uniform standards for documentation of clinical services
- Lack of standardized technical platforms to support EHR
- Low support for startup expenses or reimbursement for implementation costs
- Insufficient planning
- Poor communication
- Inadequate oversight and coordination of implementation efforts
- Deficiencies with vendor support
- Loose interpretation of regulatory requirements
Regardless of the implementation’s size, problems that typically emerge during such projects include:

- Disconnected communication between leadership and departmental personnel
- Specificity of operational workflow designs that do not have sufficient detail
- Training and communication initiatives are not adequately considered and/or planned
- Project plans and issue tracking tools are not utilized effectively to facilitate overall project management/oversight initiatives
- Formal approval checkpoints for appropriate operational representatives are not incorporated into the validation process
- The determination of security configuration requirements are made loosely or too late
- Insufficient testing is performed
- The configuration of application controls is not sufficiently considered

With the increased focus on technology across the healthcare industry, organizations should ensure implementations are managed proactively rather than repaired reactively or delivered insufficiently.

These are exciting, while understandably challenging, times for the healthcare industry. The need for a willingness to adapt and to embrace cultural change within your organization is perhaps more important now than ever before. The HITECH Act is geared towards facilitating sweeping change throughout the industry – from encouraging the implementation of EHRs to tightening the privacy and security of patient information. The PCI DSS and FTC’s Red Flags Rules are also becoming increasingly important to our day-to-day lives.

Unfortunately, there is no checklist for compliance, no repository of “right” answers. Collaboration and knowledge sharing will be important to this process of change. While we are expected to begin addressing the HITECH Act immediately, HHS has reserved the right to clarify guidance, re-define requirements, or generally just change its mind in the months to come. The healthcare industry will have to respond accordingly. While compliance with the Red Flags Rules has been delayed a second time, and the guidance clearly states that it is merely intended to be a starting point, those programs must be put in place and operating effectively in the very near future. Also, we should expect to hear more and more about healthcare organizations insufficiently addressing the requirements set forth by the PCI DSS. And surely your organization does not want to be the first big headline cited for a breach. Proactively addressing each of the areas outlined in this article may be critical to your organization’s continued success as we are thrust into this new era of change.


KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.