Top 20 IT Risks for the Healthcare Industry - and How to Mitigate Them

Raj Chaudhary, CRISC, CGEIT, and Robert L. Malarkey, CISSP, CISA

Moving into 2015, the healthcare industry continues to undergo dramatic changes and, in turn, evolving risks. With the increasing role of technology in all aspects of healthcare, from administrative practices to patient care, it's no surprise that industry leaders often rank IT-related risks at the top of their concerns.

These concerns are not misplaced. An evaluation of risk assessments conducted by CHAN Healthcare, a subsidiary of Crowe Horwath LLP, during the first six months of 2014 uncovered more than 800 risks related to IT across 13 health systems in 33 states. Based on two primary factors in determining healthcare organizations' risk profiles – strategic and business impact and business environment complexity – the following risk areas have been identified as the top 20, running from the most to least significant. Some of these might not yet be on every organization's radar, but they probably should be.

1. Health Information Exchanges

As health information exchanges (HIEs) make patient information electronically available across organizations within a region, community, or hospital system, privacy and data security concerns have become paramount. The risks are compounded by the numerous systems and organizations involved. To give all of the organizations using an HIE confidence in the data security practices, it's important to establish a common security framework to be used consistently across the organizations.

2. Meaningful Use

Meaningful use (MU) poses a major risk for both hospitals and providers because of the substantial funds tied to satisfying the MU criteria. With Centers for Medicare & Medicaid Services (CMS) audit activity showing no sign of relenting, healthcare organizations are understandably worried about being adequately prepared. To reduce the odds of adverse audit findings, organizations should formally assign accountability for MU attestation to an internal or external team charged with gathering and maintaining the necessary documents to comply with the attestation requirements. Organizations that take a more informal approach to attestation can find that vital components, like security risk analyses, fall between the cracks, leaving the organizations in the unfortunate position of potentially being required to refund CMS payments.

3. Data Warehousing

Data-based business intelligence is quickly moving to the forefront for most healthcare organizations. The greater the emphasis on better managing outcomes and overall population health, the more important data (clinical or otherwise) becomes. It's essential, therefore, that a healthcare organization maintain a secure data warehouse where the data is both available and accurate. The data interface, whereby data transfers from a hospital system to the warehouse, must be equally secure and accurate to minimize any risk.

4. ICD-10 Transition

The transition to International Classification of Diseases (ICD)-10 will have a far-reaching effect across healthcare organizations, but some organizations have taken the latest extension of the implementation deadline as a cue to slow-walk or even suspend their preparation. That's a mistake. Significant pre-implementation training and testing are necessary to confirm that claims will be properly coded and transmitted when the transition occurs on Oct. 1, 2015.

5. Accountable Care Organizations and Clinically Integrated Networks

Accountable care organizations (ACOs) received much greater attention in risk assessments in the first half of 2014 compared with the prior year. Most organizations now are involved in ACOs or clinically integrated networks (CINs) in some way, and risks continue to multiply as participating organizations are forced to share data. As with HIEs, data security and privacy are critical, and participants are concerned about issues such as liability for data breaches (discussed later) and the vulnerability of the organiza-

tions with which they are joining forces in an ACO or CIN. Ideally, consistent security, privacy, and related practices will be hashed out and agreed upon during due diligence and negotiations.

6. Disaster Recovery and Business Continuity
Productivity, revenue, and even patient safety could be severely affected if systems and data are not available and operational at all times. While business continuity related to disaster recovery is not a new concern for healthcare organizations, it ranked high because of its strategic and business impact. The good news is that once an organization performs a business impact analysis of all of its critical systems, it will have a better road map for how best to prioritize critical systems and respond when disaster strikes.

7. Biomedical Devices
Unidentified security vulnerabilities in biomedical devices can affect patient safety as well as the privacy of data on devices and networked systems. To combat the risk of these sophisticated computers being hacked, they must be kept up to date with security patches issued by vendors and manufacturers. Antivirus software should be current, too.

8. System Implementation
Many healthcare organizations are susceptible to risks related to the implementation of electronic health record, financial, and other business systems. Organizations frequently have had tight deadlines for implementing systems, but key controls nonetheless must be established. Post-implementation audits also should be performed to confirm that the relevant system was implemented in accordance with management's intentions regarding issues such as change management, security, user access, and encryption.

9. HIPAA Security
With data security frequently in the news, the Health Insurance Portability and
Accountability Act (HIPAA) remains an area of significant risk for healthcare organizations. Maintaining the security of protected health information is challenging, and readiness for Office of Civil Rights (OCR) audits is a common concern. Organizations must have comprehensive policies and procedures in place to comply with HIPAA requirements, including technical, physical, and administrative safeguards. Those policies and procedures should be regularly evaluated and updated as necessary, and they must be enforced. Supporting documentation demonstrating adherence to policies should be retained.

10. Asset Management and Software Licensing
Many organizations have issues with tracking not only their physical IT assets but their software licenses as well. Lack of control in these areas can lead to financial losses for the organization. For example, without a centralized asset management system that keeps a complete inventory of IT assets, the assets easily can disappear with disgruntled employees or as a result of inadvertent mistakes by well-meaning employees. To avoid losses related to software licensing, the organization must stay on top of exactly what it has paid to license and how it actually is using the software. An organization that deploys software among more employees than are covered by its license risks litigation with the licensor. And an organization that purchases greater licensing rights than necessary is throwing away money.

11. IT Governance
IT leadership must establish adequate policies and procedures and involve stakeholders from other departments in decision-making. Steering committees should govern IT aspects of major initiatives such as ICD-10, MU, and major clinical application implementations. Everyone – and every project – across the organization must adhere to the same IT requirements. If they don't, problems can arise behind the scenes that could force the organization into the costly position of scrapping a project and starting over from the beginning. Also, a lack of enforcement of established requirements could cause repeat general computer control issues over time due to inconsistencies.

12. Network Security
Network systems might not have the requisite integrity or could be vulnerable to loss or failure due to external or internal attacks or threats. The result could be unauthorized access to or theft of sensitive information or crashes that prevent access to critical systems and applications, with negative consequences to both patient safety and staff productivity. Organizations must protect their networks with security measures including redundancy, firewalls, access restrictions, and patches.

13. Data Loss Prevention
Electronic protected health information (ePHI) and similarly sensitive data can be disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. All confidential data stored on workstations, laptops, and other mobile devices must be identified, accounted for, and secured, with triggers and alerts set for potential disclosures or breaches when data exits via an open end point (for example, downloaded via USB or external hard drive). This includes confidential data that is in the possession of contractors.

14. Third-Party Vendor Oversight
The growing prevalence of third-party vendors in healthcare has expanded organizations' potential liability. Organizations must verify that their vendors comply with the organizations' policies and procedures as well as with the applicable legal requirements. Compliance responsibilities should be spelled out in service agreements, and organizations should monitor vendor performance. When dealing with overseas vendors to whom data will flow, healthcare organizations at a minimum must see that data is encrypted and background checks are conducted for vendor employees who will have access to the data.

15. Mobile Devices
Security for mobile devices that connect to an organization's network, system, or data is critical for protection of ePHI. Mobile device management solutions that enforce identity management, device registration, and encryption should be considered, as should a "bring your own device" (BYOD) strategy if employees will be able to access e-mail and other systems on personal devices. If an organization adopts a BYOD policy, it must have mechanisms in place to prevent access to critical data and deal with the loss of personal devices, such as the ability to perform a remote wipe.

16. Project Management
Numerous competing IT priorities must be effectively managed in order to avoid cost overruns and late project completion. But the project management office (PMO), which typically takes the lead on implementation of large systems, sometimes fails to provide such management. Conversely, the IT department sometimes goes around the PMO and does its own thing. Both groups must treat all projects equally and consistently.

17. Interfaces
With numerous system implementations going on, there is increased risk that interfaced data flowing between systems is not accurate and complete. Interface issues can adversely affect patient care and revenue recognition. Tools must be developed to promptly identify data flow errors and alert personnel to the issues. The human element is required to monitor logs and the results of transfers and to then respond to errors on a timely basis.

18. System Access and User Provisioning
Unauthorized access to data or applications is a significant organizational risk, making system access a highly ranked area of concern. Healthcare organizations often struggle to maintain consistent core controls (for example, passwords, timeouts, and lockouts) around system access, particularly given the speed with which they are implementing new systems and Web-based portal applications. Provisioning – or granting the right type of access to the right user – also has come up regularly in healthcare organizations' risk assessments. As with system implementations, tight deadlines and a lack of oversight and enforcement can't be allowed to usurp proper controls.

19. "Shadow IT"
"Shadow IT" refers to applications that are administered outside of the IT department (for example, by a clinical or operational department or respective individuals). These applications can lack core controls in the areas of system access, change management, and backup and recovery. It potentially could make sense for the director of radiology to provide most of the IT support for the department's system, but the director must enforce the organization's corporate IT policies and procedures. To achieve consistency, an organization must keep tabs on which systems are being supported "locally" and monitor their adherence.

20. PCI DSS
The Payment Card Industry Data Security Standard (PCI DSS) was formulated by the credit card industry's PCI Security Standards Council and applies to all entities that store, process, or transmit credit cardholder data (the latest version took effect Jan. 1, 2015). The standard, which outlines technical and operational system requirements to protect cardholder data, often is overlooked in the healthcare industry. To avoid fines and liability, organizations should inventory credit card data, including all points of sale, and determine whether the data's protection satisfies the standard based on the organizations' merchant level.

The Best Defense Is a Strong Offense
The first step to minimizing the top IT risks facing healthcare organizations is to undergo a risk assessment to validate controls and flag concerns and gaps. These risks are pervasive across the healthcare industry, but those organizations that take a proactive stance to uncover and mitigate them are less likely to suffer potentially devastating financial and reputational losses.

Raj Chaudhary is a principal with Crowe Horwath LLP in the Chicago office. He can be reached at 312.899.7008 or raj.chaudhary@crowehorwath.com.
Rob Malarkey is a director with CHAN Healthcare, a subsidiary of Crowe, in the Englewood, Colo., office. He can be reached at 720.874.1240 or rob.malarkey@crowehorwath.com.