Washington Healthcare News

wahcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

VOLUME 4, ISSUE 5 MAY 2009

Personal Health Information: Compliance and Security

By Chris Kradjan
Partner
Moss Adams LLP and
Practice Leader
Information Technology Auditing and
Consulting Group

Estimates indicate that close to 1 in 5 hospitals have experienced an information breach in the past six months, and surveys suggest that 1 in 23 individuals have been the victim of identity theft. Compromised personal health information (PHI) is indeed a real risk, and thanks to increased public scrutiny and media attention—as well as direct legal, monetary, and reputational implications—PHI compliance and security often top the list of IT projects for health care organizations.

Fortunately, administering an effective IT compliance program and enforcing PHI security do not have to be onerous when done in orchestration with other initiatives. The most progressive IT departments are working carefully to coordinate EMR implementations, routine security audits, HIPAA and PCI compliance, Red Flag Rules privacy programs, disaster recovery planning, quality control, and ITIL adoption, to name a few. By working on these various efforts in an organized manner, organizations can simultaneously address multiple risks, and do so in a more efficient and economical manner.

To address health information privacy, organizations should first consider the challenges. We can categorize these into three groups: consumer expectations, organizational and environmental factors, and technology.

Consumer expectations can come in many forms, such as interoperability, a high level of care, 24/7 coverage, and zero tolerance for PHI exposure.

Compounding factors from organizational and environmental causes include balancing a vast number of specialties with a wide array of internal and external parties, responding to similar yet disparate regulatory requirements, overcoming the absence of clear standards, staff resistance to change, and investing financial and staff resources wisely in light of restrictions.

Finally, technology constraints appear within fragmented and disparate systems, data housed in silos and data warehouses, lack of full integration, limitations on interoperability, and dissemination of data through mobile devices.

Implementation of an effective compliance and security program that protects the privacy of PHI must encompass the following:

- Data and threat identification
- Policies and procedures
- Employee training
- System security
- Compliance documentation
- Detection and reporting methodologies

While the development of a privacy program to protect PHI may originate with a subcommittee of the organization's board, the ultimate responsibility needs to rest at the top of the organization. This will establish appropriate expectations when it comes to PHI security and compliance. The board should appoint a privacy officer who administers the compliance framework and remains accountable for results. The privacy officer should serve as the first line of defense for supervising, monitoring, and staying well-versed in the many disciplines affecting compliance.

To sufficiently identify relevant data and threats, the organization should brainstorm with other institutions, consider possible threat domains, perform a risk and readiness assessment, determine system limitations, institute system controls where possible, and develop compensating safeguards as needed. This process allows for the constructive development of policies and procedures that can be cross-referenced to the various regulatory requirements, support meaningful employee orientation programs, and become the foundation for staff training content. With periodic updates, the documentation and training elements can be useful for developmental education and ongoing awareness—and for effectively communicating the board's expectations to the staff.

At the heart of protecting PHI is a thorough risk assessment. This entails isolating at-risk data elements and systems, implementing strong security settings for user roles, instituting logical structures of protection to system records, and using logging features within systems. When automated controls are not available, organizations should develop manual procedures and controls to compensate for inherent system limitations. Interaction with peers will prove critical in jump-starting this endeavor and avoiding having to reinvent the wheel.

Once effective compliance and security systems are in place, management must work collectively to provide sufficient staff awareness around the program as well as streamline and centralize reporting so that identified issues are captured, triaged, and appropriately addressed. In larger organizations, this is often best done through coordination between the IT, internal audit, and compliance teams. Given the need for transparency under many of the current regulations, organizations should ensure that identified breaches are properly addressed and reported through a controlled response plan, communicated to consumers for notification purposes, and meet external reporting requirements.

Chris Kradjan is a Partner with Moss Adams LLP and the Practice Leader for the Information Technology Auditing and Consulting Group. He has been with Moss Adams since 1994, and has been consulting since 1992. Chris specializes in providing service to health care organizations, not-for-profit, government and private businesses. His consulting engagements have involved the use of state-of-the-art methodologies and tools for analysis, planning, estimating costs, scheduling, and risk management for proposed solutions. Mr.

Kradjan can be reached by phone at 206-302-6511 or by email at chris.kradjan@mossadams.com. To learn more about Moss Adams LLP visit their web site at www.mossadams.com.

Reprinted with permission from the Washington Healthcare News. To learn more about the Washington Healthcare News visit wahcnews.com.