Advancing HIM and Privacy Roles Through Information Governance

Save to myBoK

By Katherine Downing, MA, RHIA, CHPS, PMP

Healthcare organizations are under constant attack from cybercriminals due to the richness of information they collect, store, and disseminate that can also be used for multiple types of fraud and identity theft. Stolen credit card information only lasts until the victim cancels the card, but healthcare data has an extended lifespan. The ability to monetize the information stored across healthcare organizations has proven easier and more effective than other industries, so the decade of the healthcare hack will continue. Despite increased IT budgets and protections, healthcare organization breaches continue, and due to HIPAA and HITECH disclosure requirements, frequently make the news.

The breaches in healthcare have dire implications for organizations, who spend an average of $4 million on breach investigation, mitigation, and credit protection, according to the 2016 Ponemon Institute's "Cost of a Data Breach Study."[1] The study also reports that the cost incurred for each lost or stolen record containing sensitive and confidential information increased from a consolidated average of $154 to $158. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent.

Since the original interpretation and implementation of the HIPAA Privacy Rule in 2003 and HIPAA Security Rule in 2005, privacy and security officers have been leading, educating, and auditing compliance with the rule and organizational policy. As HIPAA compliance becomes more and more "business as usual," organizations are seeing less of a need for a facility-level privacy officer. And often, that role has moved to a market- or division-level privacy role that has oversight over more than 10 hospitals. This shrinking of a facility-level role for privacy has left somewhat of a vacuum as AHIMA members look at AHIMA's Health Information Career Map and their available paths in organizations.

This change in scope of the privacy officer is partly because little has changed in the HIPAA Privacy and Security Rules, especially since the HITECH implementation in 2009. Without major regulatory changes, education becomes limited to standard HIPAA training on an annual basis, which is an industry best practice. Additionally, new employees typically undergo HIPAA training when they're onboarded. This is much less frequent than when HIPAA was new in 2003 and 2005, when HIPAA training happened on a weekly or monthly basis. The good news is that privacy and security is a key competency in governing information, and, therefore, the health information management (HIM) leader with privacy expertise is positioned well in the organization to lead the effort.

In organizations successful with information governance (IG), the privacy and security audit committee or privacy and security compliance committee is often the committee that takes on the role for steering IG. This committee typically has the right representation and a compliance focus that makes the IG transition easier. The committee also has a lot of crossover as illustrated in the sidebar below.

Member Crossover Between IG Committee and Breach Response Teams

Information Governance Committee Resources used: AHIMA's IG Toolkit 2.0	**Privacy/Security Breach Response Team**[2] Resources used: AHIMA's Breach Management Toolkit
Members: Medical staff Health Information Management Security Officer Privacy Officer Quality Nursing	**Members:** Medical staff Health Information Management Security Officer Privacy Officer Quality Nursing

Finance Legal Compliance Risk IT Decision support Research Clinical Informatics	Finance Legal Compliance Risk IT

IG Expands Current Privacy, Security Practices in Healthcare

Information governance is a program that serves healthcare organizations by expanding the view of privacy and security efforts from just protected health information to all information sources and points of access across the organization. Information governance also seeks to improve quality, patient safety, and population health by bringing together information resources and aligning them to strategic and operational needs. Healthcare data is expanding exponentially, and the details can make or break a healthcare organization. With the right governance strategy, information from that data can help make the right decisions across every area of an organization, including classification of information and ensuring security.

AHIMA's definition of IG is "an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements." Information governance is not a new concept—it is just new to healthcare. Other industries such as banking, finance, the military, and pharmaceuticals have all been embracing information governance as they have been dealing with Big Data for much longer than healthcare. Healthcare is just now under pressure from the explosion of data in electronic health record (EHR) systems and the exponential increase of information access points through mobile devices, patient portals, accountable care organizations, and health information exchange.

Some of the benefits of IG include lower costs, reduced risk, more accurate payments, and better regulatory compliance. The ability to use information for advanced analytics can result in a competitive advantage in the market. Most leaders across healthcare realize that their data and information is not as trustworthy and reliable as it should be. When a HIM professional asks how taking over coding for outpatient has affected billing, they might hear "We have increased payments per patient by $6 but we can't be sure that is due to the HIM department taking over coding."

In other words, the data just isn't as trustworthy as it needs to be to make business decisions. Most leaders and users of information are proponents of using data as an asset, including: chief information officers (CIO), chief medical information officers (CMIO), HIM professionals, privacy officers, security officers, compliance officers, and health lawyers. These individuals can therefore become likely allies of an IG program that focuses on better protecting and securing information while also better leveraging data as an asset.

Getting Started with IG

Larger healthcare organizations that have performed an information governance maturity assessment have been able to move swiftly. AHIMA's Information Governance Adoption Model™ is the only model for assessing IG maturity in healthcare. Assessment helps because information governance is such an all encompassing effort that organizations need to determine which projects take priority.

There is still a long way to go across the healthcare industry with assessment, understanding, acceptance, and adoption of information governance. Healthcare leaders know it is needed, they are just under pressure from different initiatives and they don't always realize that IG can assist across the organization in many ways. Record retention and legacy systems are often areas where IG initiatives can result in cost savings for the organization. Data governance initiatives can start to move quality into information capture, access, and use across the entity. Policies and practices for e-mail, social media, mobile devices, and text messages are often areas of initial focus.

What Does IG Cost?

Organizations are not adding staff or significant costs to implement an information governance program. Successful organizations are using existing staff and projects that result in return on investment to show initial success with IG efforts. Information governance initially requires education and understanding of the benefits. From that point it really "clicks" with healthcare leaders that IG processes are necessary and will benefit not only the organization and its business partners but ultimately the patients and a provider's entire population.

Information governance projects in healthcare are succeeding, and HIM leaders as well as privacy officers are great options for leadership and the chief information governance officer role. Ultimately information governance initiatives are going to increase patient safety and quality of care through the ability to share trusted, reliable, accurate information with patients and clinicians. Adopting an IG program shows an organization's commitment to managing its information as a valued strategic asset.

Notes

1. Ponemon, Larry. "2016 Ponemon Cost of a Data Breach Study: Global Analysis." *SecurityIntelligence*. June 15, 2016.
2. Downing, Katherine. "Navigating a Compliant Breach Management Process." *Journal of AHIMA* 85, no. 6 (June 2014): 56-58.

Katherine Downing (kathy.downing@ahima.org) is senior director of information governance at AHIMA.

Article citation:
Downing, Katherine. "Advancing HIM and Privacy Roles Through Information Governance" *Journal of AHIMA* 88, no.2 (February 2017): 26-27.