Addressing Privacy and Security Risks in Today's Healthcare Ecosystem

Save to myBoK

By Ann Meehan, RHIA

Information is a healthcare organization's most strategic asset and requires enterprise-wide management to ensure that it is protected and secured in the most compliant way—for patient care and other business purposes. More than ever, healthcare organizations face growing challenges in managing information due to the ever-growing volume of information, evolving regulatory requirements, and increasing risks associated with security threats.

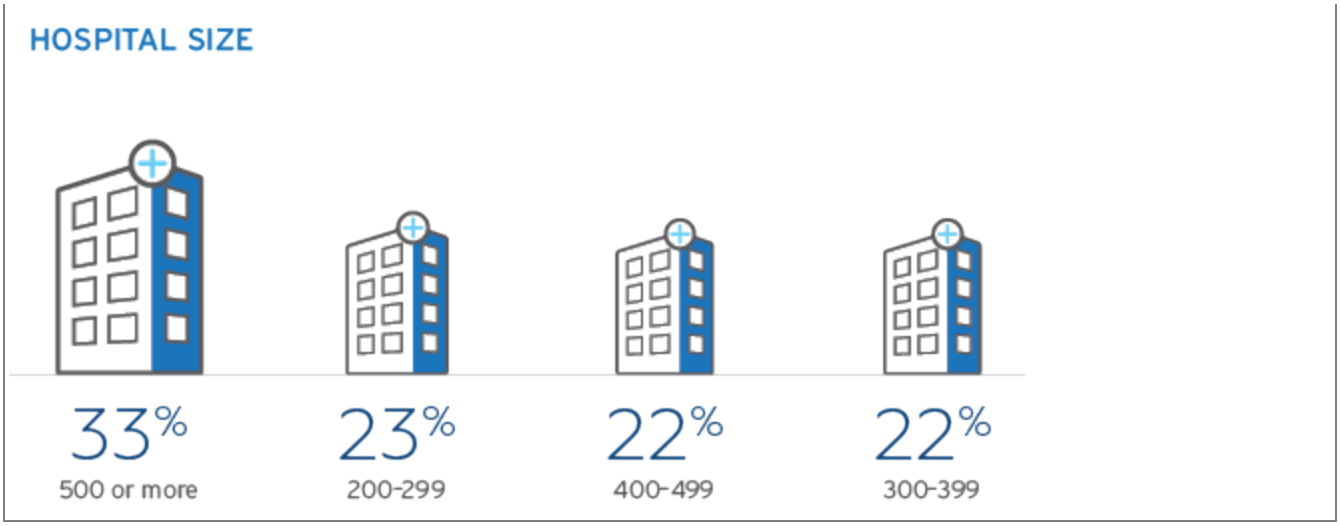
A recent survey of 100 healthcare compliance leaders by Iron Mountain resulted in insights that health information management (HIM) professionals can leverage to better prepare their organizations to address privacy and security risks in this challenging ecosystem.

The key goals of the study were to:

1. Identify compliance leaders' most pressing priorities over the next three to five years.
2. Review industry trends hindering progress.
3. Explore how information governance (IG) can help advance identified priorities and improve privacy and security enterprise-wide.
4. Assess the current state of IG across three high-impact areas that are indicative of an organization's risk profile and IG program maturity. These areas include:
    - Information Inventory and Integrity
    - Retention Policy Management and Defensible Disposition
    - Privacy and Security
5. Explore best practices that can help compliance leaders address common gaps to advance IG, support strategic priorities, and enable enterprise-wide compliance.

Interviews were conducted from December 2017 through February 2018 and included hospital compliance and privacy leaders across a range of bed sizes (see Table 1 below). Survey results were published in a white paper.[1]

Table 1: Survey Respondents' Bed Sizes



Healthcare Compliance: Goals and Priorities

When asked what their top three compliance priorities are, respondents indicated:

1. Standardize policies and processes governing the management, use, security, and release of protected health information (PHI) across the organization and/or newly acquired/recently merged facilities (75 percent)
2. Employee compliance training and education (62 percent)
3. Enable HIPAA compliance and prepare for OCR audits (41 percent)

Interestingly, these three priorities are very much interconnected. The need to standardize is at the heart of ensuring consistency in how information is managed and secured. Without a standardized approach, it would be virtually impossible to effectively manage hardcopy records and electronic records and information in today's complex, ever-changing healthcare ecosystem. Without workforce training and education, a standardized approach is not possible. Additionally, lack of employee awareness or adoption of standardized processes inhibits an organization's ability to be compliant and meet audit requirements.

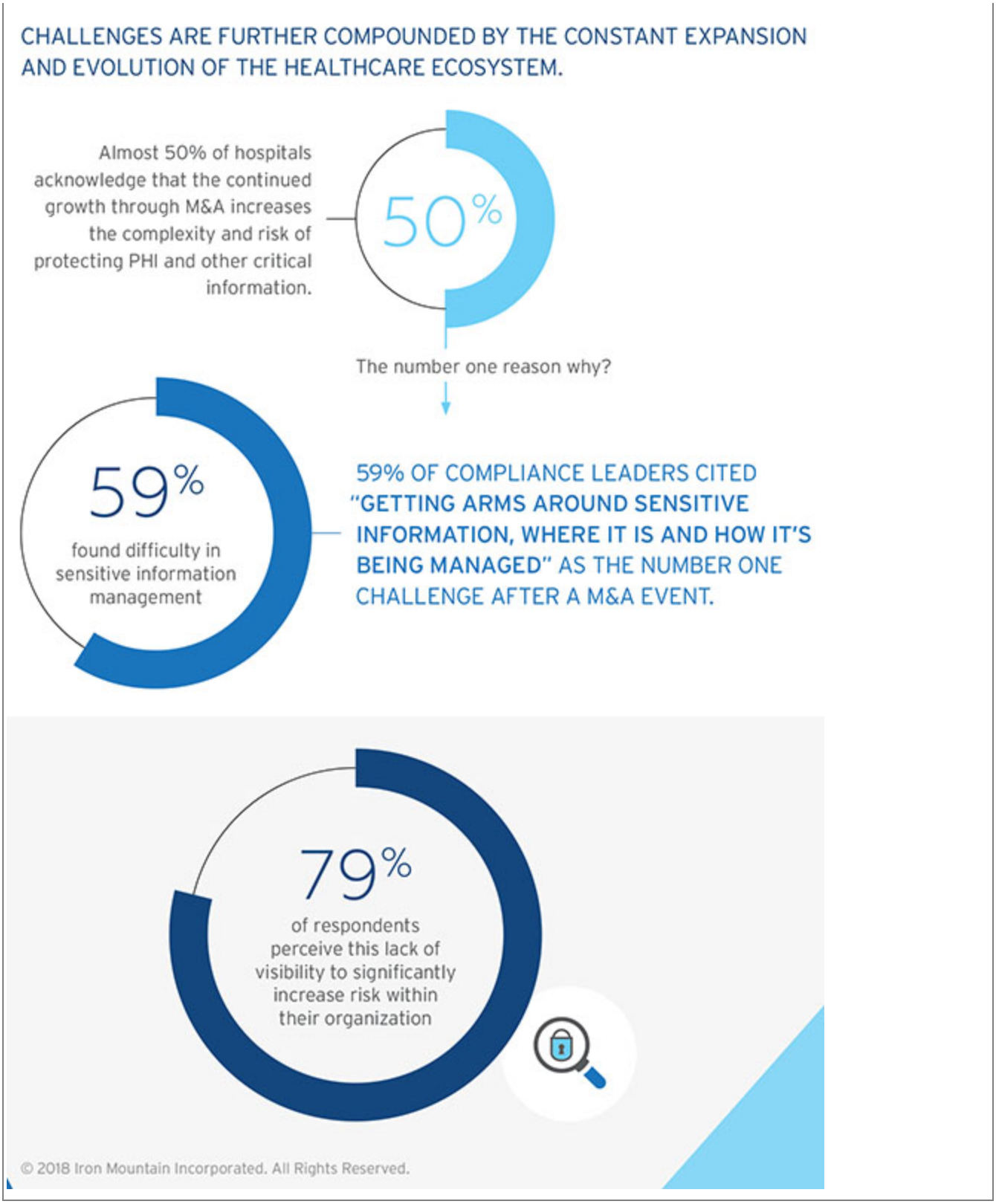
Barriers to Success

Survey respondents were also asked to identify the biggest barriers to success. The top barrier at 33 percent was accelerating employee understanding and acceptance of compliance, which ties back to the previously reported need to provide employee training and education. Along with that comes the need to monitor adherence to role-specific compliance requirements learned and reinforced during training and the ability to hold staff accountable.

The second-biggest barrier to compliance identified by the survey, at 29 percent, are the challenges associated with convincing the medical staff to embrace change. The medical staff is an important audience for education around privacy and security policies and procedures. Organizational silos impeding visibility into facility or department processes represents another barrier. While this was reported by only 16 percent of respondents, it's a very real challenge across all healthcare organizations where decisions and management of information are often driven at the department or business unit level, resulting in disjointed and non-compliant processes. All this increases the risks associated with the protection and security of information.

Table 2 below outlines the next set of insights gained in the white paper. The table speaks to the continued growth of information due to merger and acquisition (M&A) activity. Fifty percent of hospitals noted that the growth of information due to M&A activity makes it very challenging to protect PHI and other critical information.

Table 2: Merger and Acquisition Challenges



As noted by 59 percent of organizations, this is due to the difficulty in understanding where information is, how it's used, and how it's managed. The lack of information visibility increases the risk around information protection and security, as indicated by 79 percent of respondents. These insights indicate that healthcare organizations need a way to know exactly what information is captured, generated, used, reported on, and stored. In other words, healthcare organizations need to manage the lifecycle of their information.

Could Information Governance Be the Answer?

Standardization and education are consistently identified as mission-critical priorities throughout the white paper. These initiatives are also foundational components of an enterprise-wide IG program. Let's quickly recap what IG is.

AHIMA defines information governance as: "An organization-wide framework for managing information throughout its lifecycle and for supporting an organization's strategy, operations, regulatory, legal, risk, and environmental requirements."[2] It is strategic in nature and includes policies, procedures, and education that are enterprise-wide and that address all types of information in all formats.

High Impact Areas of IG

As it relates to addressing privacy and security risks, industry experts believe there are three sub-components of IG that are high-impact areas. These include: Information Inventory and Integrity; Retention Policy Management and Defensible Disposition; and Privacy and Security. HIM professionals work in these areas every day, making HIM subject matter experts for each area and providing the perfect opportunity to lead these initiatives or provide consultative advice.

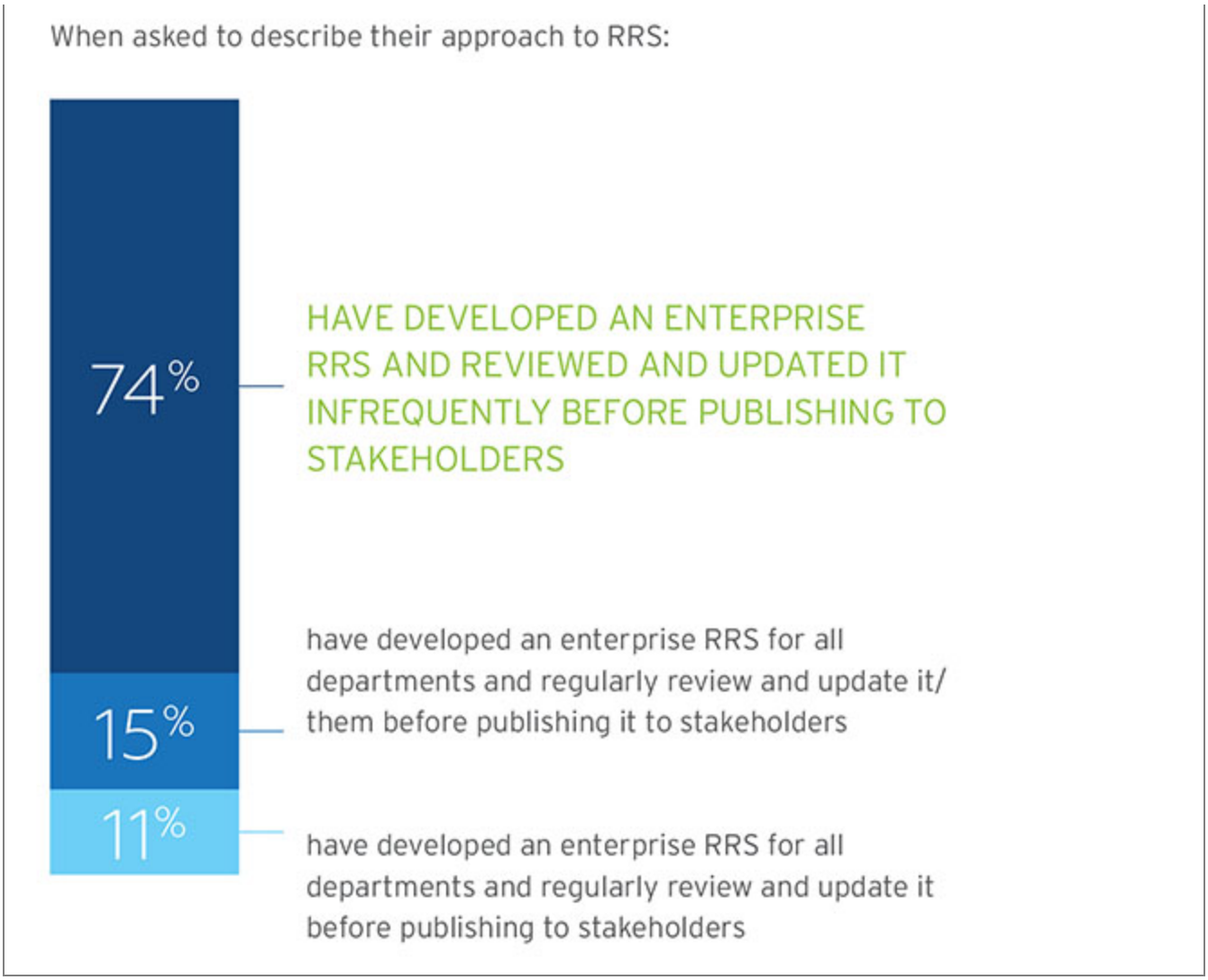
Beginning with Information Inventory and Integrity, protecting information is based on knowing what you have and where it resides. Healthcare organizations should capture basic data elements of its information in an Information Inventory. Equally important is the integrity of the information that the healthcare organization maintains.

An example that all HIM professionals can relate to is the accuracy of the enterprise master patient index (eMPI). Does your organization proactively prevent duplicate eMPI creation? Does your organization consistently monitor for and address any duplicates or overlays that are created and correct any downstream systems affected? Are trends captured to identify why duplicates are created, and is education provided to ensure duplicates are eliminated or at least minimized? Additionally, does your organization calculate the percentage of duplicates created? HIM professionals know the ramifications of duplicate MPI, including patient care errors and inadvertent disclosures.

Moving onto the second-highest impact area, Retention Policy Management and Defensible Disposition, each healthcare organization needs a record retention schedule and policy that is consistently updated, readily understood, and easily enforced, and which addresses all types of records across the organization—including electronic data.

Table 3 below provides a summary of survey results indicating that 74 percent of organizations have an enterprise-wide record retention schedule but it is not updated frequently.

Table 3: Enterprise-wide Record Retention Schedules (RRS)



HIM professionals are the guardians of the patient medical record and have an obligation to not only ensure that the record is accurate and complete, but that it is retained for the timeframe required by federal and state regulations. Equally important is that HIM professionals ensure patient medical records are destroyed when they meet the timelines in those regulations and no longer serve a business purpose. Defensible disposition is the defined processes around the appropriate disposition of paper and electronic data to prevent the legal discoverability of that information, reducing the risk of breaches.

This brings us to the last of the high-impact areas, Privacy and Security. Physical safeguards and access management are vital to ensuring that information is protected and classified appropriately. Many healthcare organizations have paper records that were created prior to implementing an electronic health record (EHR). Until those records can be destroyed, they have to be protected by securing them in storage locations that are environmentally appropriate, effectively secured through access controls, and accessed by only those with a legitimate need to do so. Another area that falls into this high-impact area is release of information (ROI) practices. HIM professionals should know: Who is performing ROI? What training is provided to ROI staff to ensure the appropriate handling of PHI?

HIM professionals are at the center of disclosure management. Many HIM directors serve as privacy officers as well and have a crucial role in compliance by ensuring that approved policies and procedures are in place and followed to identify data breaches, reporting requirements, and follow-up, including sanctions.

HIM and IG Strengthen Privacy and Security

HIM professionals play a key role in ensuring compliance to address privacy and security risks. Information governance practices facilitate compliance requirements through enterprise-wide policies and procedures around all workflows and tasks, including MPI management, ROI, and defensible disposition.

"Information governance provides a sustainable, foundational framework that drives the cross-functional awareness and the accountability required to proactively identify and remediate policy gaps and emerging risk across the organization," wrote the authors of the white paper.[3]

Using information governance practices, HIM professionals can work to ensure that the healthcare organization's most valuable asset is protected and secured and that the organization can get strategic value from its information.

Notes

1. Iron Mountain. "Healthcare Compliance: Leveraging Information Governance to Address the Growing Privacy and Security Risks in Today's Ever-Evolving Healthcare Ecosystem." 2018. www.ironmountain.com/resources/whitepapers/h/healthcare-compliance-survey.
2. Cohasset Associates and AHIMA. "2014 Information Governance in Healthcare Benchmarking White Paper." www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Benchmarking.ashx.
3. Iron Mountain. "Healthcare Compliance, Leveraging Information Governance to Address the Growing Privacy and Security Risks in Today's Ever-Evolving Healthcare Ecosystem."

Ann Meehan (ann.meehan@ironmountain.com) is a senior consultant at Iron Mountain.

Article citation:
Meehan, Ann. "Addressing Privacy and Security Risks in Today's Healthcare Ecosystem." *Journal of AHIMA* 90, no. 3 (March 2019): 32–35.