Information Governance’s Privacy and Security Component

Save to myBoK

By Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA

In the most simple terms, information governance is the accountability framework and decision rights employed by an organization to ensure effective and efficient use of information across the enterprise. Ideally, this also achieves enterprise information management (EIM), which is the infrastructure and processes that ensure all of an organization's information is trustworthy and actionable.[1] For an organization to be successful it is critical that it treats information as an asset. Information governance practices embody the idea of information as an asset. It is an overall management strategy that starts with executive leadership and infiltrates down and throughout the organization.

Information governance, which also encompasses data governance and information technology governance, is becoming increasingly important to health information management (HIM) as health information exchange becomes more widespread and, in turn, brings large volumes of outside data into systems. It is important to note that information governance, together with data governance and information technology governance, helps organizations identify, understand, control, and appropriately exchange data.

Therefore, privacy and security issues must be considered as part of any information governance initiative. Given their foundation of knowledge in privacy and security, HIM professionals are well-equipped to help healthcare organizations develop information governance strategies. Specifically they can help organizations determine why a governance strategy is necessary, who must be involved, and which resources will be the most helpful. A successful information governance strategy will ultimately influence and help secure the integrity of the information.

Keeping Information Trustworthy and Controlled

HIPAA placed a spotlight on the confidentiality, privacy, and security of protected health information (PHI) over a decade ago, and the spotlight will remain there long into the future. There are major governance and cultural differences among healthcare organizations based on type, philosophy, and approach to privacy and security. Although compliance with pertinent laws and other external requirements are undoubtedly important, governance is more about how that compliance is implemented. Governance must take into consideration and address a range of issues, such as: how the front desk operates and collects patient information at registration, whether policy permits remote employee access, whether laptops are allowed to leave the premises, how the qualifications and role assignment of privacy and security officers is determined, and everything in between.

Two keywords in the definition of information governance are "trustworthy" and "control." These two words are vital when implementing and instilling sound privacy and security practices throughout an organization. Like information governance, privacy and security practices must come from the top down and be woven into the culture of an organization.

As technology advances and PHI becomes more electronic, information governance and an organization's privacy and security program must work hand-in-hand to ensure effective management of the data. It takes strong collaboration between these strategies to build a positive reputation and sustain trust not only internally with users, but in the community and among individual consumers as well.

Information governance strengthens the overall quality of patient care while fostering patient safety along the way because the data is both accounted for and protected.

Getting Stakeholder Support

Once support from the executive team has been established, getting involvement and participation from all major staff stakeholders is equally critical. The privacy and security officers must collaborate to establish an effective program, starting with a committee comprising the following members, which may vary from organization to organization:

- Executive leadership
- Appointed privacy officer
- Appointed security officer
- Department/floor leader or representative
- Clinicians
    - physicians
    - nurses
    - medical assistants
    - ancillary services
- HIM staff
- IT staff
- Human resources
- Compliance/risk management
- Legal counsel

An organization may have one committee or it may have several to address the many different aspects that encompass a privacy and security program. Regardless of size, overall governance must take into account the structure of the committee(s), how policies and procedures will be managed and enforced, and requirements for training, education, and awareness. For example, an organization may choose to designate one committee to the investigation and management of privacy breaches.

The entire workforce must be trained on the policies and procedures of the privacy and security program. The training must clearly set expectations and accountability for all choices and actions made. Everyone should have a clear understanding of how to handle and manage the PHI that they come in contact with during their day.

Privacy and Security Governance Resources

Below are recommended government and AHIMA resources to help develop and strengthen a healthcare privacy and security program.

Government

- Department of Health and Human Services' (HHS) Privacy Rule: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
- HHS Security Rule: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
- HHS HITECH Omnibus Rule: http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html
- HHS and Department of Education – Federal Educational Rights and Privacy Act (FERPA): http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
- Department of Justice – Privacy Act: http://www.justice.gov/opcl/privacyact1974.htm
- Department of Justice – Freedom of Information Act (FOIA): http://www.foia.gov/about.html
- US Courts – E-Discovery – Federal Rules of Civil Procedure: http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Civil%20Procedure.pdf

AHIMA

- AHIMA Analysis of the Final HITECH Omnibus Rule: http://bok.ahima.org/PdfView?oid=106127
- Privacy and security focused Practice Briefs found in the HIM Body of Knowledge (new or updated in 2013; available at www.ahima.org):

  - A HIPAA Security Overview
  - Breach Risk Assessment Best Practices
  - HIPAA Privacy and Security Training
  - Notice of Privacy Practices
  - Patient Access and Amendment to Health Records
  - Retention and Destruction of Health Information
  - ROI for Marketing and Fundraising
  - Sanction Guidelines for Privacy and Security Violations
  - Securing Wireless Technology for Healthcare
  - Security Risk Analysis and Management: An Overview
  - Security Audits of Electronic Health Information
  - The 10 Security Domains
- Toolkits found in the HIM Body of Knowledge (free to AHIMA members):
  - Information Integrity in the Electronic Health Record
  - The Release of Information Toolkit

Creating a Sound Privacy/Security Program

There are many state and federal laws surrounding security and privacy compliance of PHI. Most federal laws set the floor, not the ceiling, and state laws vary tremendously. Accreditation agencies—such as the Joint Commission—and government initiatives—such as the "meaningful use" EHR Incentive Program—play a compliance role as well.

At a minimum, privacy and security officers developing and managing privacy and security programs should be familiar with the following regulations:

- Clinical Laboratory Improvement Amendments
- Federal Rules of Civil Procedure (E-Discovery)
- Freedom of Information Act
- Federal Educational Rights and Privacy Act
- Health Insurance Portability and Accountability Act
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Genetic Information Nondiscrimination Act
- USA Patriot Act of 2001
- Privacy Act of 1974
- State laws (where applicable)
- United States Code Title 42

A sound privacy and security program is only successful if its individual pieces are also successful. The elements of a flourishing program will vary by setting, size, and type, and the number of policies and procedures will vary as well as the methods of training offered. Continuous monitoring of the program will identify problem areas and gaps in education as well as compliance needs.

The core elements of a sound privacy and security program should include:

- Strategy
  - Executive and stakeholder support
  - Embed into annual performance evaluations
  - Regular review and updates to ensure success
  - Appointed privacy and security officers
- Privacy and security committee

  - Meet regularly
  - Stay abreast of industry and regulatory changes
  - Regulate and enforce compliance/sanctions
  - Evaluate issues/determine solutions
- Policies and procedures
  - Access/electronic access
  - Accounting of disclosures
  - Breach investigation and management
  - Business associate agreements
  - Disclosure and sale of health information
  - Employee activation/termination
  - Marketing/fundraising
  - Minimum necessary
  - Notice of privacy practices
  - Release of information
  - Research
  - Requested restrictions
  - Sanctions
- Education and training
  - Provide resources (i.e., manuals, access to the laws, electronic tutorials)
  - Face-to-face training sessions held at orientation and on a regular schedule
  - Online training sessions offered year round
  - Help line/help desk
  - Reminders (i.e., e-mail alerts, posters)
  - Recognition weeks (i.e., fairs, prizes, and organizational activities)
  - Newsletters
  - Mock audits

Alongside the elements that make up a privacy and security program, governance plays a role in how decisions are actually made regarding an organization's privacy and security practices. Governance plays a critical role in the "one size does not fit all" design that is the backbone of meeting privacy and security compliance.

The HIPAA Security Rule was created to be "scalable" and "technology neutral." Together, HIPAA Privacy and Security Rules apply to all types of PHI that exist on paper or electronic records. It is ultimately up to the organization to determine how to apply those laws and meet all requirements.

Organizations must remember that when implementing a program, governing it must take into account the size and type of the organization, but also the financial needs, the types of technology being used (i.e., mobile devices versus desktop computers), staff needs (i.e., who will investigate breaches), and the policies that support each decision.

Note

1. AHIMA. "Information Governance." 2013. http://www.ahima.org/topics/infogovernance.

Angela Dinh Rose (angela.rose@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Rose, Angela Dinh. "Information Governance’s Privacy and Security Component" *Journal of AHIMA* 84, no.11 (November 2013): 54-56.