Information Protection Framework: Data Security Compliance and Today's Healthcare Industry

Executive Summary

Today's Healthcare industry is facing complex privacy and data security requirements. The movement from paper to digital records of health information is accelerating, making it ever more important that information be protected. Organizations must be equipped with an information protection strategy that is inclusive of Security, Privacy, Risk Management solutions.

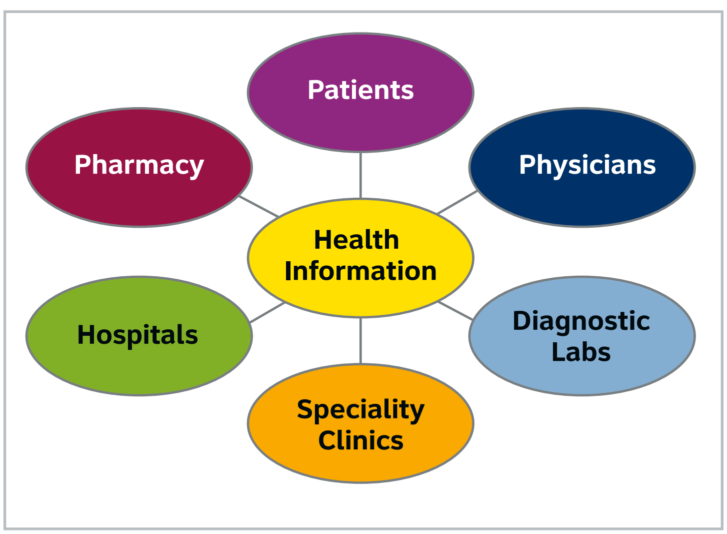
Over the last several years, a number of laws and regulations have been adopted which impact the use of information in the health industry[1]. The Health Information Technology for Economic and Clinical Health Act ("HITECH"), part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), was signed into law with the goals of developing a healthcare IT infrastructure, encouraging entities to adopt Health Information Technology ("HIT") and to "meaningfully use" Electronic Health Records ("EHRs"), and to protect the privacy of the consumer. ARRA also modified the Health Insurance Portability and Accountability Act ("HIPAA") in several ways: it made portions of HIPAA directly applicable to Business Associates; it gave patients broader rights to an accounting of disclosures, including those for Treatment, Payment and Operations ("TPO"); it modified and expanded obligations for breach notifications, both by Covered Entities and Business Associates; it strengthened the privacy rights of patients; and it gave certain federal and state entities greater authority over-compliance and enforcement.

This legislation and associated regulations require affected entities to do a variety of things, such as:

- Review and potentially modify their privacy and security policies
- Implement and update employee training programs
- Develop breach notification protocols
- Maintain and follow internal audit plans
- Modify existing data sharing arrangements that are no longer permissible
- Be prepared for external audits

Healthcare Information Flows

The flow of healthcare information follows the patient; starting at the doctor's office, to laboratories, imaging centers, pharmacies, and other care facilities. This natural flow of medical records provides many points where information security must be considered and proper processes implemented.



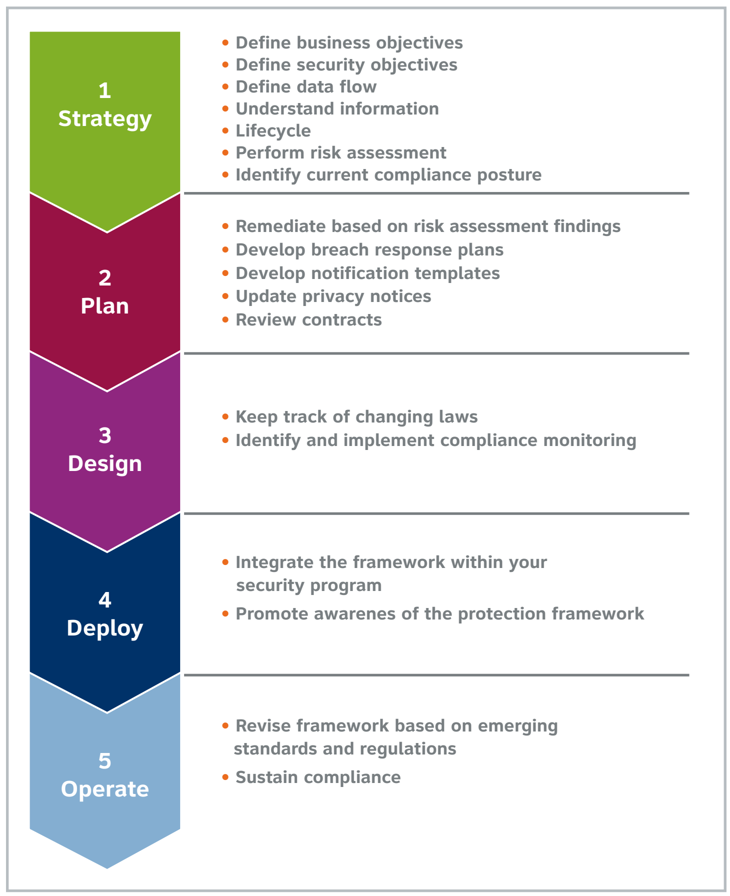
The increasing interconnection, while extremely beneficial for patient healthcare, also raises risks related to patient privacy and confidentiality. There is a heightened consumer awareness regarding privacy of sensitive information, and the potential impact of reported data breaches has caused consumers to expect and demand protection of their personal health information.

As healthcare operations benefit from advancing technologies which promote information sharing, it is necessary to build and use the appropriate information protection framework to preserve the integrity and protect the confidentiality of Protected Health Information ("PHI") and Personally Identifiable Information ("PII").

Information Protection Framework

To enable effective and secure information sharing, healthcare organizations require a transparent, consistent ability to identify information sensitivity and determine proper handling. This is achieved by developing an information protection strategy and framework that is comprehensive, but flexible enough to meet changes in healthcare infrastructure while achieving compliance requirements. As many organizations have learned, focusing on one set of compliance requirements at a time does not assist in building a comprehensive framework or strategy; it only increases the amount of time and resources which organizations have to spend on meeting requirements.

The information protection strategy/framework should look at a broad set of protection requirements including specific internal security and privacy requirements, risks to the business, applicable compliance requirements, and industry standards.



Key Elements of the Health Information Protection Framework

Risk Management: Integral to Security and Compliance

Healthcare organizations are required to conduct risk assessments as per the HIPAA Security Rule on a periodic basis to identify data security risks and implement appropriate security controls for their particular organization and can use the resources that have been provided by the Department of Health and Human Services (HHS) as a good starting point.

Healthcare organizations must perform ongoing risk assessments to identify the risks that could compromise their data, and determine what the potential effects of the risk could be based upon the environment in which they operate[2]. This can guide healthcare organizations in making intelligent and informed decisions about how to allocate security resources to protect customer or patient data and ensure compliance.

Adopt a well-defined risk assessment framework that can help you identify and address the risks that are pertinent to your organization.

Risk assessment in general has many definitions in the industry today. Some view risk assessment as merely a checklist/questionnaire and consider it to be a one-time effort. Others have a deeper view of risk assessment and consider it to be a useful tool in identifying the controls that need to be put in place to maintain the security posture of the organization. In today's business operations, where information is critical to the success of a business, a solid risk assessment framework must be place in order to help with efficient risk management.

Risk in this context can be defined as the impact and likelihood of an adverse event. With respect to healthcare data, the impact and likelihood of an adverse event depends on the amount and sensitivity of the health information and the number of people or systems having access to that information. For example, an individual physician's office with one system, not connected to a network storing sensitive health information, creates less exposure and decreases the risk of the information being compromised, while a large medical provider with an extensive health information exchange infrastructure and various members accessing and handling the information creates a greater risk of the information being compromised.

Establish an information risk management program which allows your organization to address strategic and technical risks to information security.

Risk Management: Guidance

The Health & Human Services Office of Civil Rights (OCR) published draft guidance to help healthcare organizations understand what is expected of them in doing a risk analysis of their patient's PHI. The Office of Civil Rights has issued draft guidance on risk assessments[3]. The HHS Office of the National Coordinator (ONC) also produced a security practice guide for small health care practices[4] that serves as a primer for health care providers who need to understand the basic security considerations relevant to their practices. The guidance material also includes a number of references to more detailed information and further guidance.

The Office of Civil Rights calls risk analysis the "first step" to identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the HIPAA security rule.

People, Process and Technology: Key Elements of Security and Compliance

Companies handling Protected Health Information/Personal Identification Information (PHI/PII) should perform an architectural and program review to understand how their existing controls can be utilized to address identified risks before making new investments. When determining the best information protection strategy, they should review their current healthcare infrastructure to understand existing measures and processes. There should be ways to optimize, reduce costs, or minimize upcoming investments. For every compliance initiative, there are technologies that promise to provide the easiest method of complying with the requirements. Most likely, companies already have some of the technologies in place to satisfy the other compliance initiatives such as Payment Card Industry-Digital Security Standard (PCI-DSS), Sarbanes-Oxley Act (SOX), or the Gramm-Leach-Bliley Act (GLBA). Before moving forward, determine a strategy to address compliance requirements using both technological and strategic solutions. Not all requirements can be solved by technology; some are best solved with organizational and operational processes.

Develop an information protection strategy for security and compliance with the right combination of people, processes, and technologies to address your organizational risks.

Data Security: Common Thread Across the Industry

Healthcare organizations face a great variety of risks to the security and confidentiality of data and information. Applications and their supporting infrastructure create efficiency, but can also create conflicts between data sharing and data security and confidentiality. The prudent healthcare enterprise in the process of automating application modules must consider system-wide security and confidentiality across application boundaries.

Each organization must determine the level of security and confidentiality for the varying categories of information, including which access to each category of information is appropriate for the user's job function.

Before analyzing security controls, take a step back to understand what data is actually needed to support the business, how that data must be shared, and where that data is stored. Look at operations, the flow of data into, throughout, and outside of the organization, and the risks associated with the entity's current business model. This will result in an understanding of the exposures that the data faces, allowing prioritization of security measures.

The risk analysis guidance released by OCR also provides questions as examples that have been adapted from NIST Special Publication (SP) 800-665. These are examples healthcare organizations could consider as part of a risk analysis.

- Have you identified the e-PHI within your organization (this includes e-PHI that you create, receive, maintain or transmit)
- What are the external sources of e-PHI (for example, do vendors or consultants create, receive, maintain or transmit e-PHI)
- What are the human, natural, and environmental threats to information systems that contain e-PHI

To understand organizational privacy, security and confidentiality needs, determine:

- Which employees should have access to PHI/PII information to perform their jobs
- Mechanisms to educate and compel (via enforcement) individuals to keep sensitive information confidential
- Rules for the release of health-related information to third parties
- Physical barriers and system deterrents to secure data and data processing equipment against unauthorized intrusion, corruption, disaster, theft, and intentional or unintentional damage
- The location of sensitive data and the data lifecycle and regulatory requirements which impact the data

Breach Response: Before and After

The HITECH Act outlines a number of privacy and security provisions directly applicable to Covered Entities and Business Associates regarding breach notification, extending the requirements of HIPAA, and increasing enforcement and penalties. Sections 13402(e)(3) and 13402(e)(4) required that Covered Entities notify the HHS Secretary immediately of any breaches of unsecured PHI affecting 500 or more individuals and that the Secretary make these breaches publicly known on the HHS website. The HITECH Act Breach Notification Guidance[5] provides detailed steps on how to report a breach.

The HITECH Act defines "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." The Act includes two important exceptions to this definition for cases in which: (1) the unauthorized acquisition, access, or use of PHI is unintentional and made by an employee or individual acting under authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate, and such information is not further acquired, accessed, used, or disclosed; or (2) where an inadvertent disclosure occurs by an individual who is authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, as long as the PHI is not further acquired, accessed, used, or disclosed without authorization[6].

Data breach notification requirements are imposed by a number of state and federal privacy laws. In addition to meeting regulatory requirements for proactive data security, you must also consider reactive notification obligations in the event of a data breach. These obligations need to be considered in advance of, and not after, a data breach.

- Plan for Breach Detection: To ensure early breach detection, consider aggressive and ongoing monitoring programs that may range from IT audits to checking patient health records for inconsistencies.
- Plan for Breach Response: A detailed breach response plan should be in place. Consider vendors who provide turnkey notification services, including call centers and postal mail, which have experience creating tailored notification and advisory services for breach victims with special needs, such as age, mental health issues or physical disabilities. Remediation services for breach victims will help preserve public trust in your organization.

However, these notification procedures can largely be avoided if the PHI has been secured through one of a number of methodologies or technologies. HHS has issued guidance that specifies methodologies and technologies whose use renders information sufficiently unusable. Essentially, use of these methodologies creates a safe harbor, which results in covered entities and their business associates not being required to go through the notification procedures because the information breached is considered secured (secured PHI is unusable, unreadable, or indecipherable to unauthorized individuals).

Regulatory Drivers: Changing Regulations at the Federal and State Level

Constantly changing healthcare laws and regulations pose a governance risk. Does your organization have a strategy to identify and monitor its exposure? If your organization does not have a thorough understanding of compliance requirements, it will not be able to efficiently leverage its security initiatives to tackle ongoing regulatory demands. Remember that security does not equal compliance. So be aware of the requirements, solicit feedback and interpretation from outside experts, and develop a protection framework to meet security standards as well as compliance requirements. As an organization handling PHI, you should also have a framework in place to keep abreast of the changes to applicable regulatory requirements.

Sustain Compliance

Sustaining compliance requires identifying and remediating the IT infrastructure, governance, and communication problems on an ongoing basis. It requires enormous effort on the part of those charged with compliance, as well as coordination of the business processes and IT resources used to achieve compliance. Specifically, organizations must create a culture of compliance maintenance. This may require an organizational shift from a project mentality to a program mentality that will bring together the risk, governance and compliance initiatives, helping to pave the way for a converged compliance management program.

In developing a compliance plan for data security, following an integrated framework that addresses security, privacy, risk and compliance will result in a more manageable program that allows more efficient compliance efforts.

Information Protection Evaluation Checklist

Here is a list of questions that can help get you started with building the health information protection framework around the key elements.

- Strategy and Awareness
  - Have you developed a health information protection strategy that encompasses the key elements of HIPAA and the HITECH Act?
  - Have you performed a recent assessment to determine your compliance posture with the HIPAA Privacy/Security Rule?
  - Have you prepared security awareness programs to promote the education of Health Information Privacy and HITECH requirements within your organization?

- Information Security and Privacy
  - Have you reviewed and updated Notice of Privacy Practices to reflect changes in privacy and security policies?
  - Have you made updates to your security policies and program to reflect the changes in regulatory standards?
  - Have you evaluated the restrictions on the sale and marketing imposed by the HITECH Act?
- Security Technology and Operations
  - Have you developed a detailed Breach Notification Policy that complies with HITECH and any state law counterpart to the new federal breach notification provisions?
  - Have you evaluated access management if using EHR (individual's right to access) according to the HITECH guidance?
- Risk Management
  - Have you expanded your Business Associate Inventory to include vendors and other related services?
  - Have you updated Business Associate Agreements to include expanded new requirements?

Conclusion

While data security requirements such as HIPAA and HITECH impose mandatory requirements, many health practitioners and organizations recognize that protecting healthcare information and ensuring consumer privacy is also just good business practice that leads to satisfied consumers. The increasing exchanges of health information bring new challenges in privacy and security as the industry becomes more and more interconnected. The security and privacy of patient data is a key element in creating a secure healthcare information infrastructure. The magnitude, complexity, and dynamic nature of developments affecting the exchange of health information demand a broad and flexible information protection strategy. This information protection strategy must encompass risk management and governance policies so that people, processes and technologies can provide for the growing security and privacy requirements for proper treatment of health information.

References

1. For a more detailed discussion of recent revisions to health care legislation, visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html and http://healthit.ahrq.gov/portal/server.pt?open=512&objID=650&parentname=CommunityPage&parentid=7&mode=2&in_hi_userid=3882&cached=true

2. The required Risk Analysis implementation specification at § 164.308(a)(1)(ii)(A), obligates a covered entity to, "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

3. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html

4. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848086_0_0_18/Sma%20llPracticeSecurityGuide-1.pdf

5. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html and http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

6. See ARRA at Section 13400 (1)(B)

For more information contact an AT&T Representative or visit www.att.com/healthcare.

09/30/10 AB-1958

at&t