ARE YOU PROTECTED?
The Seven Steps to HIPAA Security
Adapted from a presentation by Ali Pabrai, CEO, ecfirst
According to some recent reports, it is not a matter of if a healthcare business will experience a cyber breach, it is a matter of when. An article in CSO magazine, “Every Company Compromised,” stated, “in a recent analysis of a quarter-million endpoint devices in 40 enterprises, every single corporate network showed evidence of a targeted intrusion but most of the activity was not yet at the most-dangerous data exfiltration stage.”

The FBI warns that the healthcare sector is vulnerable to cyber attacks. Further, healthcare has experienced 340% more security incidents and attacks than other industries.

Based on this very sobering information, every healthcare provider must ask the following question: how prepared is their organization from cyber-attacks to compromise personally identifiable information (PII) or confidential data such as electronic protected health information (E PHI)?

The two key areas that must be addressed to reduce risk are compliance mandates and cyber-attacks. In terms of cyber-attacks, an organization must consider just how prepared it is to discover and prevent cyber-attacks on a near real-time basis. They must consider whether the correct combinations of security controls are implemented and how these controls are being actively managed. If a cyber-attack takes place and a critical business application or system is compromised, will the breach be identified on a timely basis? The organization’s enterprise security plan must clearly articulate how the business will actively implement and manage security controls to ensure that the discovery and mitigation of breaches is consistently executed.

With compliance regulations, it is imperative that organizations be able to correctly identify all applicable federal and state regulations. These are not optional and any enterprise security plan must ensure these mandates are continually met. Compliance requirements should be addressed with the objective of always being audit ready.

On January 17, 2013 the U.S. Department of Health and Human Services (HHS) announced a new Final Rule to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). With the onset of the Final Rule, a primary care physician, a 25-bed critical access hospital and a large hospital health system are all held to the same standards, as well as to the same financial penalties. The cost for an organization to become compliant is much less than the penalties for non-compliance. These fines can range in the millions of dollars. In addition, the Final Rule now extends to business associates, which means that the healthcare organization is responsible for the actions of its contracted business partners, as both can be fined for violations to HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).

A breach also requires that the organization notify federal and state agencies and authorities. These government agencies upon receipt of breach notification information may review to assess the state of compliance with information privacy and security regulations. A lack of a credible compliance program may lead to a subsequent audit of the organization to review its compliance program. These government agency audits are a seven-figure risk to the organization if the compliance program is discovered to be weak.

So what can organizations do to improve and prepare for data breach prevention or post breach remediation steps? ecfirst, an Intalere partner through their strategic partnership with Konica Minolta, has developed a guide through their Seven Steps to HIPAA Security.
ARE YOU PROTECTED? The Seven Steps to HIPAA Security

THE SEVEN STEPS TO HIPAA SECURITY

Let’s look at each step in a bit more detail.

1. ASSIGN SECURITY RESPONSIBILITY

The process begins with assigning security responsibility. An organization must develop very specific job descriptions for privacy, security and compliance professionals. Part of this involves identifying the Information Security Officer and establishing reporting and accountability. The Information Security Officer has principal responsibility for activities associated with the availability, integrity and confidentiality of information related to patients, providers, employees and business in compliance with the organization’s security policies and procedures, and all applicable regulations and laws.

Although presumably well-versed in information security through education and experience, further training may be necessary. Below are just a few of the possible certifications that leaders could obtain to maximize their effectiveness:

- Registered Health Information Administrator (RHIA)
- Registered Health Information Technician (RHIT)
- Certified HIPAA Professional (CHP)
- Certified Security Compliance Specialist (CSCS)

This step also includes development of a budget. Estimates of overall budget vary widely, of course, based on the size of the organization. According to a 2014 Gartner study, worldwide spending on information security reached $71.1 billion in 2014, an increase of 7.9% over 2013, with the data loss prevention segment recording the fastest growth at 18.9%. Total information security spending will grow a further 8.2% in 2015 to reach $76.9 billion. In terms of areas for budget allocations that should be considered, facilities should cover areas including training and technology, risk analysis, supply chain security and mobile policy.

2. CONDUCT RISK ANALYSIS

As mentioned previously, a thorough, comprehensive security risk and vulnerability assessment is a necessary starting point for any program. In fact, the Office of Civil Rights (OCR) Guidance on HIPAA Risk Analysis states that, “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational…” Further, OCR states that “All EPHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. Risk analysis is the first step in that process.”

In conducting the risk analysis, entities should list every requirement of the HIPAA Security Rule, including every safeguard, standard and implementation specification, in a risk analysis format that identifies an organization’s state of compliance with the requirement, recommended remediation activity and associated risk priority. They should also seek to identify contingency requirements including a business impact analysis. Per Gartner’s definition, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations. The analysis should also include an information system activity review, which automates and consolidates audit controls. Finally, the analysis and report should be an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the board of directors.
3. DEVELOP SECURITY STRATEGY AND POLICIES

With the foundational elements set, the next steps are to begin to set strategies and policies, including the overall plan and policy documents. An important element includes the development of incident and breach management plans, policies and procedures. These plans should be layered and describe a roadmap to safeguard sensitive business information and enterprise vital assets. Organizations should also develop contingency plan documents including an IT Disaster Recovery Plan. Some elements of the plan:

- Reduce impact to day-to-day operations.
- Minimize overall disruption and damage.
- Minimize economic impact.
- Establish contingency operations.
- Provide training to personnel on emergency procedures.
- Establish plan for smooth and rapid service restoration.

4. REMEDIATE – CORRECTIVE ACTION PLAN (CAP)

Many of the recent examples of data breaches give us insight into some of the tactics that need to go into a remediation or corrective action plan. A 2014 major bank breach in which hackers compromised a flaw in the bank website and slowly siphoned customer account information was discovered as a result of a routine scan. It illustrated the ability of the organization to actively monitor critical systems. In another huge healthcare case in which 80 million customers and employees were impacted, the database that was accessed was not properly encrypted. Those are two of the tactics ecfirst recommends as part of an overall corrective action plan:

- Implement solutions for perimeter intrusion detection or prevention systems.
- Implement encryption solutions for data in motion and data at rest (must address backup media, laptops, portable media and other devices).
- Implement device and media control solutions.
- Implement identity management and authentication solutions.
- Deploy access control technology.
- Implement automatic logoff.
- Activate log-in monitoring and auditing capabilities.
- Deploy integrity control and encryption technology.
- Test contingency planning procedures

The better and more comprehensive of a plan that is in place and the quicker the incident response and willingness to work with governing entities, the greater the possibility for minimizing damage.

5. SECURE THIRD PARTIES: UPDATE BUSINESS ASSOCIATE CONTRACTS AND OTHER AGREEMENTS

The review and update of all Business Associate Contracts (BACs), as well as the list of business associates (BAs), is also an imperative step to the process. According to an April 2015 article in the Wall Street Journal, 20% of IT professionals state that insufficient vetting of vendors (business associates) was a leading cause of breach of their companies in 2014. According to HIPAA, a business associate is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the BA to protected health information. A BA also is a subcontractor that creates, receives, maintains or transmits protected health information on behalf of another BA.

The HIPAA rules generally require that covered entities and BAs enter into contracts that ensure each will appropriately safeguard protected health information. The BA contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the BA, based on the relationship between the parties and the activities or services being performed by the BA.

The changes announced to the HIPAA Security Rule expand many of the privacy and security requirements to business.

20%
associates, such as contractors and subcontractors. For example, BAs may also be liable for the increased penalties for noncompliance based on the level of negligence up to a maximum penalty of $1.5 million. Also, the definition of a BA is expanded to include entities or individuals that maintain protected health information (PHI) on their behalf, even if such entities or individuals never access the information. Based on this potential liability, it should be a key responsibility of a BA to ensure it completes a comprehensive risk analysis on a regular, pre-defined schedule.

6. TRAIN THE WORKFORCE
A security plan can only be as good, ultimately, as the people as the people who are tasked with implementing it. Healthcare providers must conduct security training for all members of the workforce, with training content addressing regulatory mandates and organizational policies. A strong training program also consistently communicates security requirements with security reminders, posters, etc.

HIPAA privacy and security rules actually require formal education and training of the workforce to ensure ongoing accountability for privacy and security of PHI. Per HIPAA, each covered entity must complete workforce education, audit its training program on a periodic basis, and ensure that all new hires are properly trained. The training program should include:

- Proper and timely training of the workforce members on HIPAA requirements, according to each member’s position.
- Implementation of periodic security updates.
- Installation of procedures for guarding against, detecting and reporting malicious software.
- Monitoring of log-in attempts and reporting of discrepancies.
- Implementation of procedures for creating, changing and safeguarding passwords.

7. EVALUATE AND AUDIT
Evaluation and audit should not be viewed as the final step, but just another step in a continuous loop of constant improvement. There should be constant assessment that all risks and vulnerabilities have been addressed, accepted and remediated. There must be verification that all compliance requirements are being met.

Organizations such as covered entities or business associates are typically affected by more than one regulation. Your organization may be subject not only to compliance, but also other regulations such as PCI’s DSS or state mandates. For this reason, it is strongly recommended that all organizations directly or indirectly affected by the compliance legislation go beyond the requirements of the regulation and implement appropriate solutions to protect not just PHI, but all vital enterprise assets and sensitive information.