Best Practices for Compliance with the Final Security Rule

Tom Walsh, CISSP

After 4 1/2 years of waiting, the final security rule was posted to the Federal Register on February 20, 2003. But even before the final security rule was released, the privacy rule required covered entities to have appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI) from any intentional or unintentional uses or disclosures [§164.530(c)(1)]. “Appropriate” and “reasonable” are the recurring themes found throughout both the privacy and the security rules. So what are “reasonable and appropriate” safeguards? By implementing some of the selected best practices outlined in this paper, covered entities can be assured that what they are doing is beyond reasonable and improve their chances of withstanding the legal challenge of the “prudent man” test.

Background
The old rule specified 24 requirements and 69 implementation features. The final security rule specifies 18 standards and 42 implementation specifications; of those, 20 are required and 22 are addressable.

“Addressable Implementation Specifications” demonstrate the government’s commitment to base the security standards on good business practices and make them flexible, scalable, and technology-neutral. This allows covered entities the freedom to choose the security controls and technologies that best fit with their size and risk tolerance. This does not permit an organization to simply ignore a security standard or implementation specification. The rule specifically states that covered entities must assess an implementation specification to see if it is “reasonable and appropriate.” Their decision will be based upon factors such as:

- Risk analysis
- Risk tolerance and mitigation strategy
- Not implement either an addressable implementation specification or an alternative security measure
- Current technologies and security controls already in place
- Cost of implementation

Cost is not meant to free covered entities from their security responsibilities; therefore an organization will be expected to bear some cost and expense in implementing the security rule, but no one expects the covered entity to go broke in doing it. It all goes back to applied reasonableness. How is an organization going to determine reasonableness in addressing an implementation specification? One approach would be to apply best practices when implementing the security rule.

Best Practices Defined
Because the security rule gives organizations flexibility, there is a demand to know, “What are best practices? And what are other organizations doing?”

Best practices are generally accepted principles and practices as determined by information security professionals. These practices are typically derived from one or more security principles such as “Least Privilege” and “Separation of Duties.” Best practices represent the high watermark for developing or implementing information security policy, practices, or tools to not only comply with regulatory requirements such as HIPAA but also to secure information resources based upon good business practices.

The remainder of this paper selectively describes some best practices in an active voice to encourage the reader to imagine them in a perfect organization. Note: Not all of the security standards and implementation specifications are addressed below.
Administrative Safeguards
Fifty-five percent of the security rule falls under administrative safeguards with 12 required standards or implementation specifications and 11 addressable implementation specifications. Administrative safeguards refer to the covered entity’s policies and procedures and other forms of documentation. Documentation used to demonstrate compliance must be retained for “six years from the date of its creation or the date when it was last in effect, whichever is later.” The standards that are grouped into administrative safeguards include: security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, and business associate contracts.

Security management process.
The security management process incorporates four required implementation specifications: risk analysis, risk management, sanction policy, and information system activity review.

“The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks.” A risk assessment attempts to answer the questions:
What needs to be protected; what are the possible threats, vulnerabilities, impact to the organization (financial and reputation), and risk tolerance of the organization; and what controls, safeguards, or countermeasures are available to protect the assets? The risk assessment is data gathering.

The risk analysis is an in-depth review of the assessment so that a covered entity can now determine which security controls, safeguards, or countermeasures it may choose to deploy and what risks it’s willing to assume based upon an analysis of the risk assessment data. The risk analysis can either be quantitative or qualitative. Since there is no such thing as 100 percent security, a good risk analysis tells the management how to best manage resources to reduce the risk to an acceptable level. This enables executive management to know the level of risk they are assuming in operating information systems in their current configurations. Executive management needs to be periodically informed of reports of information security incidents, policy exceptions, and changes in the risk profile.

Unfortunately, few healthcare organizations have conducted a formal risk analysis. Therefore, for best practices, covered entities need to look outside of healthcare for a benchmark.

In other industries, the risk analysis is a report that itemizes the critical information resources (hardware, software, information, and data) with an estimated value (generally using replacement costs) multiplied against an estimated exposure or loss factor generally expressed as a percentage.

“H ow is an organization going to determine reasonableness in addressing an implementation specification?”

This loss factor is compared against the cost to implement controls and countermeasures. If the cost for protecting the asset outweighs the cost of the estimated potential loss, then management can assume the risk. If the cost for protecting is less than the estimated loss, then management may determine it is necessary to spend the time and the money to reduce the potential loss. As a final option, management may choose to insure against the loss rather than implement any security controls.

Because threats and vulnerabilities are constantly changing, assessing and analyzing risks is an ongoing process referred to as risk management. Best practices would include conducting a limited risk assessment and analysis especially when hardware and software are upgraded or when new threats or vulnerabilities are discovered. This requires a covered entity to keep up with the latest security bulletins and configuration patches.

Assigned security responsibility.
The duties and responsibilities of a single individual must be defined and communicated to the entire workforce. The reporting structure for the information security officer commonly falls under IT (CIO), corporate compliance, internal audit, or legal. The reporting structure is not as important as influence. Influence can leverage the right people to get the job done. Therefore, an information security officer’s level of authority will help determine their level of influence within the organization. Resources such as budget and staff will demonstrate executive management’s commitment to the information security program. The two most common approaches to the role of the information security officer are that of an officer of the corporation (which means the security officer assumes some of the risks) or a consultant to executive management advising them on the risks they assume.

Workforce security. Workforce security addresses the following specifications: authorization and/or supervision, workforce clearance procedure, and termination procedures. In large organizations one of the greatest challenges is to remove users’ access in a timely fashion after they resign or no longer have need. The way to solve this problem is to have an automatic notification by the HR payroll system that notifies the IT department when an employee no longer requires access because of job change, resignation, or termination. Good business practices would also have the organization temporarily preserve the information and data files that were created by the terminating staff in the event that the manager wants to transfer those files to their replacement.

Information access management. Typically, users’ access is set up based upon another user in the organization. For example, it’s not
uncommon for IT departments to receive requests to establish Sally’s access to be just like Mary’s. The problem is Mary may be an employee who has been around for a long time and may have transferred jobs several times over her career. Each time she changed jobs, she acquired new privileges and access without having her old privileges and access revoked. Thus, the new employee, Sally, has access that far exceeds what she needs to do her job.

True role-based access would prevent this from occurring. To create role-based access, a matrix is created that lists job titles and departments against the applications and privileges needed to perform duties. By getting management and data owners to pre-approve access authorization, the IT department can establish and modify user access based upon the matrix. Service requests for additional access would be managed by exception and thus reduce the amount of paperwork a typical covered entity currently uses to manage access.

There is a policy that governs the use of temporary, group-shared, or generic user IDs. Access privileges are minimal.

Security awareness and training. In training the saying is “one size does not fit all.” The content and delivery method of a training class needs to be specifically tailored for the audience. The best way to accomplish this is by conducting a training needs assessment to ensure that each member of the workforce receives job-specific training regarding information security. The training educates users on how to select good, strong passwords and ways to remember their passwords so they will not write them down. The security training program is periodically evaluated and updated against actual organizational requirements.

New employees are required to meet a minimum training requirement prior to being granted access to clinical information systems. Even if the employee is an experienced computer user, they are still required to attend a training class and pass a competency test because each organization’s network infrastructure and policies are different. Likewise, third parties with access to organizational systems (contractors, vendors, temps, etc.) are required to complete a minimum security training.

Security incident procedures. Tracking and responding to security incidents is an important part of compliance. Many organizations have incident or occurrence reporting systems currently in place that track patient or employee safety issues. This security rule standard requires us to have a mechanism for employees to report incidents and for the organization to track those incidents.

“T o create role-based access, a matrix is created that lists job titles and departments against the applications and privileges needed to perform duties.”

Workforce members only have to call one telephone number to report any type of incident (physical security, patient unusual occurrences, safety, corporate compliance, etc.). Incidents are reported on a common form. Reported incidents are then triaged and routed to the appropriate department or person responsible.

Staff, such as Help Desk, receives special training to recognize patterns and situations indicative of incidents. An incident response team has been trained for responding to incidents and for collecting and preserving evidence in an investigation. A spokesperson has been designated and script written for responding to the press regarding security and privacy incidents.

Evaluation. Evaluation is a periodic review of technical controls and process of the entity’s information security program. An Independent Verification & Validation (IV&V) gives an objective review of the information security program to determine the effectiveness of countermeasures employed and in maintaining the systems’ security to an acceptable level of risk. Vulnerability scans of the systems connected to the internal and external network verify that systems are secure.

While the final security rule removes “certification” as a specific requirement, systems should still be certified as meeting minimum-security requirements prior to connecting to the network or processing patient information. For example, the certification process can ensure that systems are properly configured (“hardening”) and tested before being placed into production by verifying such things as the system default passwords were changed.

The certification process must be handled by qualified individuals familiar with generally accepted security guidelines and principles. To maintain “separation of duties,” the person responsible for certifying systems is not the same person responsible for implementing the security controls of the system.

Business associate contracts and other arrangements. Business associate contracts are leveraged to establish rules of engagement for vendors who have remote access to systems that store or process patient information. These agreements go beyond non-disclosure and confidentiality agreements. Specific security procedural or technical requirements and non-performance sanctions are explicitly stated in agreements.

Physical Safeguards

Physical safeguards represent 24 percent of the security rule with four required standards or implementation specifications and six addressable implementation specifications. Physical safeguards apply to facility access controls, workstation use and security, and device and media controls.
SECURITY

Access control and validation procedures. All workforce members are required to wear picture identification badges and use their ID badges to gain access into restricted areas such as the Data Center and Medical Records (Health Information Management). The use of these card swipe badges or proximity badges allows granular access control (day of week, time of day, etc.) and generates access logs (audit trails) to restricted access areas. Access requests to doors with the approvals/denials is documented and maintained for the duration of the individual’s employment or duration of relationship for contractors.

Authorizations for contractors, vendors, or consultants are verified prior to access. They sign confidentiality agreements or non-disclosure agreements and have their pictures taken using digital cameras for a visitor ID badge. The visitor badges have an expiration date printed on them.

Workstation security.

Workstations use biometric authentication with single sign-on to authenticate users. When a user steps away from the workstation, their proximity badge locks that user’s session. Because the workstation supports multiple logon sessions, another user walks up to the workstation and can log on without getting access to the previous user’s session.

Workstation monitors are positioned to keep patients and visitors from viewing the screen. When the workstations cannot be relocated, privacy screens, anti-glare screens, or screen savers are installed.

Transcriptionists or coders working from home have two internal hard drives to boot from — one for work that belongs to the covered entity and one for personal use.

Media re-use. Hard disk drives and other types of non-volatile memory are sanitized by overwriting the media at least three times with random patterns of “1’s” and “0’s” before they are reused or disposed of to prevent accidental disclosure of PHI or company-sensitive information.

Data backup and storage. On-site backup tapes are stored in fireproof safes or containers that are in a physically different location than the Data Center, and at least one set of backup tapes is stored off-site in a secure location. These backup tapes are periodically tested by restoring onto a test system.

Technical Safeguards

Technical Safeguards are the products, tools, and system features that implement and enforce the covered entities’ policies. They represent 21 percent of the security rule with four required standards or implementation specifications and five addressable implementation specifications. Technical safeguards apply to access and audit controls, integrity (of information and data), person or entity authentication and transmission security.

“Data owners periodically receive an access control list of who has access to their systems and what privileges they have.”

Access control — unique user identification. Each user is assigned a unique user ID that is never reused and is not based upon the user’s name. These user IDs are uniform across systems and platforms in the organization. Systems prohibit concurrent/simultaneous access of the same user ID.

Automatic logoff. Applications processing PHI have automatic time-outs set for 10 minutes. After five unsuccessful logon attempts in a row (e.g., user incorrectly enters their logon information — user ID and/or password), the system locks the user account forcing the user to call the Help Desk to re-enable their user account.

Audit controls. Data owners periodically receive an access control list of who has access to their systems and what privileges they have. Users are randomly selected for audit and the audit data is provided to their managers for approval of the users’ activities. Warning banners that obtain the user’s consent to auditing or monitoring are displayed at login to any system or network and contain the phrase “No Expectation of Privacy” in the banner message. Audit logs are stored on a separate system and only the Information Security Officer has access to the logs, and an automated tool is used to evaluate audit trails.

Intrusion detection systems are installed to monitor for possible external attacks to the network and a host-based intrusion detection system triggers an alarm if a user attempts to access information beyond his or her authorization.

Person or entity authentication.

There are limitations and parameters controlling the type of password that users may select (reuse, length, composition, etc.). Or strong passwords are created by the IT department and delivered to users in a sealed envelope during the new hire orientation or after the user completes their mandatory training.

The network authentication system locks the user account after five unsuccessful logon attempts in a row. If the user’s account or passwords need resetting, the Help Desk first verifies the identity of the caller and then notifies the user’s manager by e-mail that their employee’s password was reset. If the manager gets too many of these e-mails, it may also indicate an employee performance issue.

Transmission security. Best practices for network security dictate that “Deny” rather than “Allow” is the default policy on network systems. This implies that unused firewall ports should be closed unless there is documentation as to why it is opened, the time frame it will remain open, the requestor, and the manager who approved the change. The network is periodically scanned for vulnerabilities.

Other network practices include encrypting wireless transmissions, identifying modems, and verifying that they serve a specific business
need that cannot be met by any other means. When modems are used in conjunction with remote access software (such as pcAnywhere), they are properly configured to prevent unauthorized access.

**Configuration Management**

The final security rule removed the requirements for security configuration management, but it is still good business practice. Most organizations today are practicing some form of change control that is just one aspect of configuration management. Listed below are some other best practices for control and managing the configurations of information systems.

- There is a Configuration Management, Change Control Committee, or similar forum for reviewing and approving all changes to the production environment that also includes changes to operating systems and hardware. Prior to approving a change control, verification is made to see if the changes require user documentation updates such as training materials issued to users. For example, screens and options displayed may have changed as a result of upgrading an application making the training materials or quick reference guides outdated.
- As part of the change control process, the requestor indicates on the change control paperwork if the Disaster Recovery Plan (DRP) needs updating. This ensures that as the computing environment changes, the DRP stays current.
- Automated procedures are in place for updating workstation applications and anti-virus software. This system also conducts an inventory of executables running on the desktop, thus detecting if unlicensed software has been installed.

**Conclusion**

The security rule allows covered entities a great deal of flexibility in applying security safeguards based upon the organization’s size, complexity, technology, and its risk analysis. While applying best practices will not guarantee 100 percent security or compliance, they will provide a high water mark for a covered entity to achieve. Those covered entities that meet or even exceed these best practices have a level of confidence that their Information Security Program will withstand the scrutiny of a survey or review team.

Keep in mind that as technologies change (as they always do), so too will best practices. Information security is a journey not a destination.

**Authentication**

Three methods of authentication:
- Something you know (Password, PIN, mother’s maiden name, passphrase)
- Something you have (ATM card, smart card, token, key, swipe card badge)
- Something you are (biometric — fingerprint, voice scan, iris scan, retina scan)
- Combinations of any two are considered two-factor authentication.

**NOTE:** User ID and password is NOT two-factor.

**About the Author**

Tom Walsh is a Certified Information System Security Professional and a senior consultant with CTG HealthCare Solutions.