HIPAA Security Series

7 Security Standards: Implementation for the Small Provider

What is the Security Series?

The security series of papers provides guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement a provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series contains seven papers, each focused on a specific topic related to the Security Rule (see left panel). The papers are designed to give HIPAA covered entities insight into the Security Rule and to assist them with implementation of the standards. This series explains specific requirements (provisions of the rule), and possible ways to address those provisions.

CMS recommends that all covered entities read the first paper in this series, "Security 101 for Covered Entities" before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation and maintain an ongoing security program. This seventh paper in the series is devoted to implementation of the Security Rule standards, implementation specifications and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers. It assumes the reader has a basic understanding of the Security Rule.

Background

Identity theft, stolen computer disks, malfunctioning computers, hackers, and other preventable losses of information - these are just a few of the hazards facing all businesses that receive, store, and transmit data in electronic form. Many health care providers too face these same hazards. Much of the electronic protected health information (EPHI) they hold is critical to their business and vital to the care of their patients. Providers face major problems if their patient's sensitive information is stolen, misused, or unavailable.

The HIPAA Security Standards provide a structure for covered entities (health plans, clearinghouses, or covered health care providers) to develop and implement policies and procedures to guard against and react to security incidents. The Security Rule provides a flexible, scalable and technology neutral framework to allow all covered entities to comply in a manor that is consistent with the unique circumstances of their size and environment.

All covered entities must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to EPHI (see 45 C.F.R § 164.302.). Small providers that are covered entities have unique business and technical environments that provide both opportunities and challenges related to compliance with the Security Rule. As such, this

paper provides general guidance to providers such as physicians and dentists in solo or small group practices, small clinics, independent pharmacies, and others who may be less likely to have IT staff and whose approach to compliance would generally be very different from that of a large health care system. It is important to note however, that this paper does not define a small provider, nor does it prescribe specific actions that small providers must take to become compliant with the Security Rule.

The objectives of this paper are to:

- Help small providers understand the Security Rule standards, implementation specifications, and requirements as they relate to their organization.
- Provide sample questions and scenarios that small providers may want to consider when addressing the Security Rule requirements.
- Reference industry resources that provide additional information regarding compliance with the Security Rule.

Security Rule Overview for Small Providers

To understand the requirements of the Security Rule, it is helpful to be familiar with the basic concepts that comprise the security standards and implementation specifications. The Security Rule is divided into six main sections – each representing a set of standards and implementation specifications that must be addressed by all covered entities. Each Security Rule *standard* is a requirement: a covered entity must comply with all of the standards of the Security Rule with respect to the EPHI it creates, transmits or maintains.

Many of the standards contain *implementation specifications*. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either *required or addressable*. Regardless of whether a standard includes one or more implementation specifications, covered entities must comply with each standard. Where there is no implementation specification for a particular standard, such as the "Workstation Use" and "Person or Entity Authentication" standards, compliance with the standard itself is required.

- A **required** implementation specification is similar to a standard, in that a covered entity must comply with it. For example, all covered entities including small providers must conduct a "Risk Analysis" in accordance with Section 164.308(a)(1) of the Security Rule.
- For **addressable** implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the covered entity's environment. After performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions. For example, all covered entities including

small providers must determine whether "Encryption and Decryption" is reasonable and appropriate for their environment in accordance with Section 164.312(a)(1) of the Security Rule.

- Factors that determine what is "reasonable" and "appropriate" include cost, size, technical infrastructure and resources. While cost is one factor entities must consider in determining whether to implement a particular security measure, some appropriate measure must be implemented. An addressable implementation specification is not optional, and the potential cost of implementing a particular security measure does not free covered entities from meeting the requirements identified in the rule.

Using This Resource

The tables and sample questions provided here relate to the Administrative, Technical and Physical Safeguard requirements from the Security Rule and are relevant for small providers seeking to evaluate and/or establish EPHI security practices. The tables and sample questions in this document do not represent a complete list of Security Rule requirements, but provide insight into the key HIPAA Security requirements applicable to a small provider.

HIPAA Security Series

Administrative Safeguards – These provisions are defined in the Security Rule as the "administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
SECURITY MANAGEMENT PROCESS § 164.308(a)(1) *"Implement policies and procedures to prevent, detect, contain and correct security violations."*	RISK ANALYSIS (R) *§ 164.308(a)(1)(ii)(A)* *"Conduct 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."*	Have you identified the EPHI within your organization? This includes EPHI that you create, receive, maintain or transmit. Please note that EPHI may be resident on computer workstations, servers or on portable devices such as laptops, and PDAs.
	RISK MANAGEMENT (R) *§164.308(a)(1)(ii)(B)* *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."*	What security measures are already in place to protect EPHI – this can be a comprehensive view of all measures, whether administrative, physical or technical, such as an over arching security policy; door locks to rooms where EPHI is stored; or the use of password-protected files.

HIPAA Security Series

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
	SANCTION POLICY (R) *§ 164.308(a)(1)(ii)(C)* *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."*	Have you developed, applied and implemented policies specific to violations of the security policies and procedures? If so, do they provide appropriate sanctions for workforce members who fail to comply with your security policies and procedures? (i.e., have you included your sanction policy in your workforce manual and trained your staff on the policy?)
WORKFORCE SECURITY § 164.308(a)(3)(i) *"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information."*	AUTHORIZATION AND/OR SUPERVISION (A) *§ 164.308(a)(3)(ii)(A)* *"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."*	Are the procedures used by your workforce consistent with your access policies (i.e., do people who should have access actually have that access? Are people who should not have access prevented from accessing the information?)

HIPAA Security Series

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
SECURITY AWARENESS AND TRAINING § 164.308(a) (5) (i) *"Implement a security awareness and training program for all members of its workforce (including management)."*	PASSWORD MANAGEMENT (A) *§ 164.308(a)(5)(ii)(D)* *"Implement procedures for creating, changing, and safeguarding passwords."*	Does your workforce training address topics such as not sharing passwords with other workforce members or not writing down passwords and leaving them in open areas?
CONTINGENCY PLAN § 164.308(a) (7) (i) *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*	DATA BACKUP PLAN (R) *§ 164.308(a)(7)(ii)(A)* *"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."*	Do your procedures identify all sources of EPHI that must be backed up such as patient accounting systems, electronic medical or health records, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used that contain EPHI?

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS § 164.308(b)(1) *"A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information."*	WRITTEN CONTRACT OR OTHER ARRANGEMENTS (R) *§ 164.308(b)(4)* "Document the satisfactory assurances required by this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [(the Business Associate Contracts or Other Arrangements Standard)]."	Do you have contracts in place with outside entities entrusted with health information generated by your office? If so, do the contracts provide assurances that the information will be properly safeguarded? For example, if you contract with a software vendor for your practice management system, what assurances do you have that the vendor's products are HIPAA compliant?

Physical Safeguards – These provisions are defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

SAMPLE PHYSICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
FACILITY ACCESS CONTROLS § 164.310(a)(1) *"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."*	FACILITY SECURITY PLAN (A) *§ 164.310(a)(2)(ii)* *"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."*	Do your office policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft of EPHI? These could include locked doors, signs warning of restricted areas, surveillance cameras, alarms, and identification numbers and security cables on computers.
	MAINTENANCE RECORDS (A) *§ 164.310(a)(2)(iv)* *"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)."*	Has your office implemented policies and procedures that specify how repairs and modifications to a building or facility will be documented to demonstrate that the EPHI is protected?

SAMPLE PHYSICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
WORKSTATION USE § 164.310(b) *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."*	*This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required (R).*	Do your office policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation?
DEVICE AND MEDIA CONTROLS § 164.310(d)(1) *"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."*	DISPOSAL (R) *§ 164.310(d)(2)(i)* *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."*	Does your office have a method of destroying EPHI on equipment and media you are no longer using? For example, have you considered purchasing hard drive erasure software for a planned upgrade of office computers?
	DATA BACKUP AND STORAGE (A) *§ 164.310(d)(2)(iv)* *"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."*	Do you have a process in place to create a retrievable, exact copy of EPHI before the equipment on which it is stored is moved?

Technical Safeguards – These provisions are defined as the "technology and the policy and procedures that protect electronic protected health information and control access to it (the EPHI)."

SAMPLE TECHNICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
ACCESS CONTROL § 164.312(a)(1) *"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)) [(Information Access Management)]."*	UNIQUE USER IDENTIFICATION (R) *§ 164.312(A)(2)(I) "Assign a unique name and/or number for identifying and tracking user identity."*	Do you have a process in place to assign each user of your system a unique user identifier? If so, can the identifier be used to track user activity within information systems that contain EPHI? This may or may not be reasonable or appropriate for a solo clinician where access has been granted to all office staff.

SAMPLE TECHNICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
	AUTOMATIC LOGOFF (A) *§ 164.312(a)(2)(iii)* *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*	Do your current information systems have an automatic logoff capability to ensure that unauthorized users do not access data on unattended workstations?
PERSON OR ENTITY AUTHENTICATION § 164.312(d) *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*	*This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required (R).*	Does your system require the input of something known only to the person or entity seeking access to EPHI, (such as a password or PIN) prior to granting the requested access?
TRANSMISSION SECURITY § 164.312(e)(1) *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."*	ENCRYPTION (A) § 164.312(e)(2)(ii) *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."*	Based on your required risk analysis, is encryption needed to protect the transmission of EPHI between your office and outside organizations? If not, what measures do you have in place to ensure the protection of this information? Some small providers might consider password protection of documents or files containing EPHI and/or prohibiting the transmission of EPHI via email.

Additional Requirements

Please note also that the Security Rule contains organizational and documentation requirements that must be addressed by all covered entities. Organizational requirements include standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans. Policies, procedures, and documentation requirements address how each of the requirements are documented, reviewed, updated and communicated to the workforce.

In Summary

Information security is a necessity in today's world. Preventing unauthorized use of sensitive health information is a core goal of every participant in the health care industry. The Security Rule allows covered entities, including small providers, to implement reasonable and appropriate measures that enable them to comply with the Rule.

The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.

Resources

Covered entities should periodically check the CMS website at: http://www.cms.hhs.gov/SecurityStandard/ for additional HIPAA security information and resources as they work through the security implementation process. While CMS does not endorse guidance provided by other organizations, covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations for additional information. Consider obtaining and reviewing the resources available through the Workgroup for Electronic Data Interchange (WEDI), at www.wedi.org. WEDI has numerous white papers and educational resources aimed at all types of covered entities, and many directed specifically to the smaller physician office. The National Institute of Standards and Technology (NIST) at www.nist.gov also has a wide range of documents and resources to assist to entities in understanding how to comply with the spirit of the regulation.