

XXIX. Core Security Requirements

- | | |
|---|---|
| <p>A. Introduction to HIPAA’s Security Requirements</p> <p>B. What Information Is Protected and What Entities Must Comply?</p> <p>C. General Obligations Under the HIPAA Security Rule</p> | <p>D. Flexibility of Approach: Written Risk Analysis Required</p> <p>E. What Must Be Done to Comply With the HIPAA Security Rule?</p> |
|---|---|

A. Introduction to HIPAA’s Security Requirements

On February 20, 2003, the United States Department of Health and Human Services (HHS) published the final “Security Standards for the Protection of Electronic Protected Health Information” (the security rule)¹ under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The security rule had to be implemented by April, 20 2005² (April 20, 2006 for small health plans).³ The security rule had been enforced by an agency of HHS, the Centers for Medicare and Medicaid Services (CMS), but in August 2009, HHS consolidated enforcement of the security and privacy rules under the Office for Civil Rights (OCR).^{3.1} See Section XXI for further details on enforcement.

See Section XXII for Important Definitions! Section XXII includes important information regarding the security rule, including detailed definitions of the following terms:*

- Affiliated Covered Entity
- Covered Entity
- Electronic Protected Health Information (Electronic PHI)
- Group Health Plan
- Health Care Clearinghouse
- Health Information
- Health Plan
- Hybrid Entity
- Individually Identifiable Health Information
- Organized Health Care Arrangement (OHCA)
- Protected Health Information (PHI)

Section XXIV includes other important information, including the definition of business associate.

* Additional terms that are used for purposes of the security rule (but not for the other HIPAA administrative simplification provisions) are defined in this Section XXIX.

¹ 68 Fed. Reg. 8333 (Feb. 20, 2003).

² The Preamble to the final security regulations stated that covered entities, other than small health plans, would have to comply by April 21, 2005, and small health plans would have to comply by April 21, 2006. 68 Fed. Reg. 8333, 8334 (Feb. 20, 2003). However, the regulations published in the Federal Register and the Code of Federal Regulations state that covered entities, other than small health plans, must comply no later than April 20, 2005, with small health plans required to comply no later than April 20, 2006. 68 Fed. Reg. 8333, 8380 (Feb. 20, 2003); 45 CFR § 164.318. The CMS website also lists April 20 as the compliance deadline.

³ See Section XXI for details on the definition of “small health plan.”

^{3.1} 74 Fed. Reg. 38630 (Aug. 4, 2009).

Compare Privacy and Security. The security rule and the privacy rule were intended to be compatible. HHS noted, “security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information.”* Accordingly, many believe that a consistent, seamless approach to HIPAA compliance is highly effective. To help in understanding how privacy and security fit together, text boxes in this Section XXIX will highlight similarities and differences between the security rule and the privacy rule.

* 68 Fed. Reg. 8333, 8335 (Feb. 20, 2003).

1. *Structure of the HIPAA Security Rule*

The security rule provides a flexible, scalable framework that meets the security mandates established by Congress, without always prescribing the specific means that covered entities must employ to achieve compliance. In the security rule, HHS established a set of standards and provided implementation specifications for most of the standards. Some of the implementation specifications are required. Others are addressable, meaning that a covered entity must implement the implementation specifications only if they are reasonable and appropriate under the circumstances. Even the required implementation specifications allow covered entities to tailor their security measures to fit their own specific facts and circumstances. Although the security rule does not allow covered entities to make their own rules regarding security, it does allow covered entities to make “their own technology choices.”⁴

Compare Privacy and Security. The privacy rule and the security rule differ in their general approaches to regulating. The security rule requires covered entities to implement certain security safeguards but gives covered entities significant latitude to decide how best to achieve an appropriate level of protection. The privacy rule is more prescriptive: For example, it bars all uses and disclosures other than those that the rule specifically permits or requires; it grants individuals certain rights relating to their PHI, with very specific provisions governing the actions of covered entities when individuals wish to exercise those rights; and it provides that covered entities must comply with several administrative requirements.

2. *HIPAA’s Security Requirements*

The security rule requires covered entities that maintain or transmit electronic PHI to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI, to protect against reasonably anticipated threats or hazards to the security or integrity of the electronic PHI, to protect against reasonably anticipated unauthorized uses or disclosures of the electronic PHI, and otherwise to ensure their officers’ and employees’ compliance with the security rule.⁵

Focus on Group Health Plans. This manual focuses on HIPAA compliance for group health plans, the employers that sponsor them, the insurers that provide coverage to them, and the third-party administrators (TPAs) that provide administrative services to them. This Section XXIX does not attempt to provide all of the guidance that medical providers or clearinghouses need to comply with HIPAA’s security and administrative simplification rules.

⁴ 68 Fed. Reg. 8333, 8343 (Feb. 20, 2003).

⁵ SSA § 1173(d)(2); 45 CFR § 164.306(a).

3. Overview of the HIPAA Security Rule

The security rule establishes the standards and implementation specifications for PHI that is transmitted by, or maintained in, electronic media.⁶ The security rule covers the administrative, technical and physical security measures that covered entities are required to take with regard to maintenance and transmission of electronic PHI.⁷

The security rule, like the privacy rule, applies directly to “covered entities”⁸ (i.e., health plans, health care clearinghouses, health care providers that transmit certain health information electronically, and endorsed sponsors of the Medicare prescription drug discount card—see Section XXII for more details).⁹ It applies indirectly, by contract, to business associates of covered entities and requires business associates to pass their obligations through to their agents and subcontractors that handle electronic PHI¹⁰ (see Section XXIV).

Compare Privacy and Security. Both the privacy rule and the security rule require covered entities to enter into business associate contracts with third parties who qualify as business associates, although the specific provisions required in those contracts have some differences. The same definition of “business associate” applies under both the security rule and the privacy rule.

The security rule also applies indirectly, by plan amendment, to group health plan sponsors that receive electronic PHI (other than summary health information, enrollment and disenrollment information, and information disclosed pursuant to an authorization) from the plan and requires the plan sponsors to pass their obligations through to their agents and subcontractors that have access to the electronic PHI (see Section XXIII).¹¹

Compare Privacy and Security. Both the privacy rule and the security rule require amendments to plan documents if the plan sponsor desires access to electronic PHI, although the specific provisions required in those amendments are very different.

The security rule’s protections extend to electronic PHI only—it does not apply to nonelectronic PHI or to electronic information that does not contain PHI (see Section XXII for more information on what constitutes electronic PHI).¹²

Compare Privacy and Security. Both the security rule and the privacy rule protect electronic PHI. The privacy rule goes further and applies to PHI in any medium—electronic, paper, or oral.

The security rule requires covered entities to implement and maintain written policies and procedures, maintain written records of all actions, activities, and assessments that are required to be documented, and maintain the documentation for at least six years from the later of the date of its creation or the date it was last in effect.¹³

Violation of the security rule can result in significant penalties, particularly as a result of the tiered increase in the amount of civil money penalties enacted under the American Recovery and Reinvestment Act of 2009 (ARRA) (see Section XXI).¹⁴

⁶ See 68 Fed. Reg. 8333, 8334 (Feb. 20, 2003); see also 45 CFR § 160.103 (definitions of electronic protected health information, protected health information, and electronic media).

⁷ 45 CFR §§ 164.308 (administrative safeguards), 160.310 (physical safeguards), and 160.312 (technical safeguards).

⁸ 45 CFR § 164.302. The security rule uses the same definition of “covered entity” used by the privacy rule.

⁹ 45 CFR § 160.104.

¹⁰ 45 CFR §§ 164.308(b) and 164.314(a).

¹¹ 45 CFR § 164.314(b).

¹² 45 CFR § 160.103 (definition of electronic PHI).

¹³ 45 CFR § 164.316.

¹⁴ American Recovery and Reinvestment Act of 2009, § 13410(d), Pub. L. No. 111-5 (2009).

Compare Privacy and Security. The same penalties that apply to violations of the security rule apply to violations of the privacy rule.

CMS Enforcement Approach. CMS was asked what enforcement action might be taken against a group health plan that had complied with the HIPAA privacy rule but had done nothing to comply with the HIPAA security rule. CMS representatives responded, informally, that upon receiving a complaint, CMS would contact the plan administrator (or whomever had legal authority over the plan) by letter, indicating that a complaint had been filed and requesting comments. CMS then would conduct an investigation based on the complaint and the plan's response. If CMS found that nothing had been done to comply with the security rule, it would discuss with the plan corrective action and a compliance timeline. If the plan had performed a risk analysis but did not have a written report of the risk analysis, the plan would need to contact the entity that performed the risk analysis and obtain a written report or recreate the risk analysis and write a report.*

It is not clear whether this enforcement approach will be followed in the future, particularly in light of the enhanced enforcement provisions enacted under ARRA.† Also, as of August 2009, HHS delegated responsibility for the enforcement of the security rule from CMS to OCR.‡ See Section XXI for further information on enforcement.

* ABA Joint Committee on Employee Benefits, Technical Session Between the Centers for Medicare and Medicaid Services and the Joint Committee on Employee Benefits, Q/A-3 (May 1, 2006), available at <http://www.abanet.org/jceb/2006/CMSQA2006.pdf> (as visited Aug. 10, 2009).

† American Recovery and Reinvestment Act of 2009, § 13410, Pub. L. No. 111-5 (2009).

‡ 74 Fed. Reg. 38630 (Aug. 4, 2009).

B. What Information Is Protected and What Entities Must Comply?

1. What Information Is Protected by the HIPAA Security Rule?

The HIPAA security rule¹⁵ applies to electronic PHI, which is defined as PHI that is transmitted by, or maintained, in electronic media.¹⁶ In turn, “electronic media” is defined as:

- (a) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- (b) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.¹⁷

The security rule requires a covered entity to protect its electronic PHI, regardless of where it resides or is accessed. A covered entity must protect its electronic PHI even if the electronic PHI resides on devices or media owned by others or on media or devices owned by a covered entity that travel off the covered entity's premises. A covered entity is also responsible for the protection of electronic PHI that may be accessed from off its premises. Of particular concern are laptops, home-based computers, personal digital assistants, smart phones, USB flash drives, e-mail, public workstations, and public wireless access points.¹⁸

¹⁵ A more complete discussion of what information is protected by the security rule is found in Section XXII and the safeguards to consider relating to information stored in electronic media or devices is found in Section XXIII. This discussion addresses only the basic elements.

¹⁶ 45 CFR § 160.103.

¹⁷ 45 CFR § 160.103.

¹⁸ *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* (Jan. 2007), reproduced behind Appendix Tab 8.

Disposal of Electronic PHI used off of the Covered Entity's Premises. The security rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. Whatever the disposal method, a covered entity must ensure that appropriate workforce members, even those working off-site, receive training on and follow the disposal policies and procedures of the covered entity. For example, the policies or procedures could require that employees or other workforce members who use electronic PHI off-site return such PHI to the covered entity for proper disposal. The covered entity should apply appropriate sanctions for failure to comply with its disposal policies and procedures.[†]

[†] HHS Frequently Asked Questions About the Disposal of Protected Health Information, Q-6 ("How should home health workers or other workforce members of a covered entity dispose of protected health information that they use off of the covered entity's premises?"), available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaq.pdf> (as visited May 12, 2009).

- *Workforce Issues.* If a covered entity permits its workforce to download electronic PHI to devices or media that are owned by the employees, or if workforce members take company-owned devices or media off the covered entity's premises or access electronic PHI from devices outside of the covered entity's control, the covered entity is responsible for the security of that electronic PHI and the covered entity's policies and procedures should address its protection.¹⁹
- *Business Associate Issues.* If a covered entity contracts with a service provider to house its electronic PHI or to perform plan functions that require electronic PHI, the covered entity must enter into a business associate contract that requires the service provider to protect the electronic PHI.²⁰
- *Plan Sponsor Issues.* If the employer that sponsors a group health plan performs some or all of the plan's administration functions and requires electronic PHI for those functions, then the plan document must be amended to require the employer/plan sponsor to protect the electronic PHI.²¹

CMS has issued helpful security guidance on the remote use of electronic PHI, emphasizing the importance of workforce training that specifically addresses risks associated with remote access to electronic PHI and includes clear instructions for accessing, storing, and transmitting electronic PHI.^{21.1} CMS also suggests policies that prohibit transmission of electronic PHI over open networks or downloading electronic PHI to public computers.²²

"Sneakernet" Is Covered. The security rule applies to "the physical movement of removable/transportable electronic storage media."^{*} This includes movement via "sneakernet," which is defined as "a method of transmitting electronic information by carrying it physically from one location to another, usually on a floppy disk or other removable medium."[†]

^{*} 45 CFR § 160.103.

[†] Encarta World English Dictionary, North American Edition, available at <http://encarta.msn.com/encnet/features/dictionary/dictionaryhome.aspx> (as visited May 12, 2009).

¹⁹ *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* (Jan. 2007), reproduced behind Appendix Tab 8.

²⁰ 45 CFR § 164.308(b).

²¹ 45 CFR § 164.314(b).

^{21.1} *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* (Jan. 2007), reproduced behind Appendix Tab 8. See also ABA Joint Committee on Employee Benefits, Technical Session Between the Centers for Medicare and Medicaid Services and the Joint Committee on Employee Benefits, Q/A-6 (May 5, 2008), available at <http://www.abanet.org/jceb/2008/CMS2008.pdf> (as visited May 12, 2009) (CMS officials indicated that as of the time of their informal, nonbinding remarks, the agency had no plans to amend the HIPAA security regulations to incorporate the previously issued written guidance on remote use of electronic PHI).

²² *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* (Jan. 2007), reproduced behind Appendix Tab 8.

Although the security rule applies only to electronic PHI, HHS has indicated that standards for the security of PHI in nonelectronic form “may be proposed at a later date.”²³ HHS also noted in the preamble to the security rule that “protected health information in paper or other form also should have appropriate security protections.”²⁴ In addition, one of the administrative requirements under the privacy rule calls for covered entities to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”²⁵ This provision applies to all PHI, not just electronic PHI. Thus, cautious covered entities may wish to review the security of all of their PHI and implement appropriate safeguards for both electronic and nonelectronic PHI.

Compare Privacy and Security. The privacy rule regulates uses and disclosures of PHI,* while the security rule regulates the creation, receipt, maintenance, and transmission of electronic PHI.† All electronic PHI is PHI subject to the privacy rule. But not all PHI is electronic PHI—PHI is the larger category and electronic PHI is the smaller. If information is not PHI, it cannot be electronic PHI, so everything that is excluded from the definition of PHI (for example, education and treatment records as defined by FERPA, and employment records held by a covered entity in its role as an employer)‡ is also excluded from the definition of electronic PHI.

* 45 CFR § 164.502(a).

† 45 CFR §§ 164.302 and 164.306(a)(1).

‡ 45 CFR § 160.103.

2. What Entities Must Comply With the HIPAA Security Rule?

a. Covered Entities

The HIPAA security rule applies directly to “covered entities,”²⁶ a term that is defined as (1) health plans; (2) health care clearinghouses; (3) health care providers that conduct certain types of transactions in electronic form;²⁷ and (4) endorsed sponsors of the Medicare prescription drug discount card.²⁸

Most single employer group health plans (and some multiemployer group health plans) are “virtual entities”—they exist as an entity, if at all, only in the form of documents. They have no workforce, no hardware, no software, no premises, no facilities and no electronic information systems. How can they “have” PHI or electronic PHI when they have no place to put it and no one to take care of it? The agencies regulating HIPAA have stated that an ERISA group health plan is a legal entity separate from the employer that sponsors it (because the plan can be sued under ERISA) and separate from other entities that may perform services for it,²⁹ and a group health plan doesn’t require a workforce, hardware, software, premises, facilities, or electronic information systems in order to exist and to “have” PHI and electronic PHI.³⁰ Of course, if a group health plan is a virtual entity, then someone else must be holding and taking care of its PHI and electronic PHI. Under the HIPAA privacy and security rules, the three entities that can constitute the “someone else” are business associates, insurers, and the employer that sponsors the group health plan. The group health plan may allow a business associate to create, receive, maintain, and transmit electronic PHI if there is a business associate contract in place that complies with the security requirements, and it may allow the employer/plan sponsor to do the same if a plan amendment that complies with the security requirements is in place. No business associate agreement is required between a health plan and an insurer.

If all of a group health plan’s electronic PHI is held by business associates, insurers, or the employer that sponsors the plan, then it seems that the group health plan’s obligations under the security rule may be limited to those standards and implementation specifications that do not address workforce, hardware,

²³ 68 Fed. Reg. 8333, 8342 (Feb. 20, 2003).

²⁴ 68 Fed. Reg. 8333, 8342 (Feb. 20, 2003).

²⁵ 45 CFR § 164.530(c).

²⁶ Additional information on this subject is found in other Sections of this manual. Section XXII contains a complete discussion of “covered entities.” Section XXIII discusses in more detail the obligations of employers/plan sponsors that perform administrative functions for the group health plans they sponsor. Business associates and business associate contracts are discussed in Section XXIV.

²⁷ 45 CFR §§ 160.103 and 164.104.

²⁸ SSA § 1860D-31(h)(6)(A); 42 CFR § 403.812(a).

²⁹ 65 Fed. Reg. 82645 (Dec. 28, 2000).

³⁰ This reasoning, even if correct for ERISA plans, is flawed because HIPAA regulates non-ERISA group health plans (such as plans sponsored by local governments and churches), which in virtually all instances are not legal entities at all, but just written descriptions of certain benefits provided by employers to employees, like an employee handbook describing vacation benefits for employees.

software, premises, facilities, or information systems. What's left? Appointment of a security officer, performance of a risk analysis (which would determine that all electronic PHI is in the hands of business associates or the employer/plan sponsor), development of risk management procedures (which would be limited because all electronic PHI is in the hands of business associates or the employer/plan sponsor), periodic evaluation to determine whether anything has changed that would require a change in the risk analysis or risk management procedures, and ensuring that business associate contracts or a plan amendment (or both) are in place and comply with the security requirements. The plan sponsor's obligations under the plan amendment would then be governed by the terms of the plan amendment and, if applicable, ERISA.

What About Fully Insured Plans That Are Hands-Off PHI? The privacy rule excepts fully insured plans that are hands-off PHI from most of the privacy requirements (because the insurer has the obligations). There is no similar exception in the security rule. However, a fully insured plan that is hands-off PHI would probably also be a virtual entity, as discussed previously, and could probably limit its security obligations in the same way.

CMS representatives were asked about the applicability of certain HIPAA security requirements, such as the requirement to have a contingency backup plan, if a group health plan has no electronic PHI on-site and a TPA maintains all of the group health plan's electronic PHI. The CMS representatives responded informally that the group health plan could rely on the TPA's backup plan, but suggested that the group health plan's written risk analysis and its business associate contract with the TPA should both note that the plan is relying on the TPA's backup systems.³¹

A More Conservative Approach to Compliance. Some group health plan advisors take a more cautious view of the obligations of group health plans that have no workforce, hardware, software, premises, facilities, or electronic information systems, and advise treating the plan sponsor's employees who perform plan administration functions as members of the plan's workforce. Under this interpretation, the plan would be considered to hold any electronic PHI that is held by plan sponsor personnel. This interpretation would require that the plan comply with each of the security standards and implementation specifications with regard to any electronic PHI held by the plan sponsor on the plan's behalf.

In the context of the privacy rule, HHS was asked specifically to "clarify that employees administering a group health plan or other employee welfare benefit plan on their employers' behalf are considered part of the covered entity's workforce."^{*} The agency declined to give a yes or no answer and instead responded by referring to some of the requirements of the plan amendment, as follows:

As long as the employees have been identified by the group health plan in plan documents as performing functions related to the group health plan...those employees may have access to protected health information. However, they are not permitted to use or disclose protected health information for employment-related purposes or in connection with any other employee benefit plan or employee benefit of the plan sponsor.[†]

Further clarification from HHS would be very welcome.

* 65 Fed. Reg. 82461, 82579 (Dec. 28, 2000).

† 65 Fed. Reg. 82461, 82579 (Dec. 28, 2000).

b. Business Associates

Effective February 17, 2010, many of the provisions of the HIPAA security rule apply directly to "business associates,"^{31.1} a term that generally encompasses an entity that performs a function or activity on

³¹ ABA Joint Committee on Employee Benefits, Technical Session Between the Centers for Medicare and Medicaid Services and the Joint Committee on Employee Benefits, Q/A-3 (May 1, 2006), available at <http://www.abanet.org/jceb/2006/CMSQA2006.pdf> (as visited May 12, 2009).

^{31.1} 45 CFR § 160.103.

behalf of a covered entity or provides certain specific services for a covered entity and has access to individually identifiable health information. See Section XXIV for a complete discussion of the types of entities that are considered business associates under HIPAA. Specifically, under ARRA,^{31.2} business associates must comply with the administrative safeguards,^{31.3} physical safeguards,^{31.4} technical safeguards,^{31.5} and the policies and procedures and documentation requirements^{31.6} under the security rule—in the same manner as those requirements apply to covered entities. See subsection E.

C. General Obligations Under the HIPAA Security Rule

Security Requirements to Apply to Business Associates. While the discussion in this subsection C relates to the obligations that apply to a covered entity, effective February 17, 2010, the same obligations apply to a business associate of a covered entity.*

* American Recovery and Reinvestment Act of 2009, § 13401, Pub. L. No. 111-5 (2009).

1. Security: General Requirements

The HIPAA security rule requires a covered entity to meet four general security requirements. The covered entity must:

- ensure the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits;³²
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information;³³
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the security rule;³⁴ and
- ensure that the covered entity's workforce is in compliance with the security rule.³⁵

The HIPAA security rule is flexible in that it requires compliance but in most instances allows a variety of security measures to achieve compliance. In deciding what security measures to use, the rule requires a covered entity to take into account:

- the size, complexity, and capabilities of the covered entity;
- the covered entity's technical infrastructure, hardware, and software security capabilities
- the costs of security measures; and
- the probability and criticality of potential risks to electronic PHI.³⁶

These requirements must be met by applying the standards set forth in the security rule and as discussed in subsection E.

^{31.2} American Recovery and Reinvestment Act of 2009, § 13401, Pub. L. No. 111-5 (2009).

^{31.3} 45 CFR § 164.308.

^{31.4} 45 CFR § 164.310.

^{31.5} 45 CFR § 164.312.

^{31.6} 45 CFR § 164.316.

³² 45 CFR § 164.306(a)(1).

³³ 45 CFR § 164.306(a)(2).

³⁴ 45 CFR § 164.306(a)(3).

³⁵ 45 CFR § 164.306(a)(4).

³⁶ 45 CFR § 164.316(b).