Summary of the HIPAA Security Rule

This is a summary of key elements of the Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) Security Rule,[2] as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act.[3] The summary addresses who is covered, what information is protected, and what safeguards must be in place to ensure appropriate protection of electronic protected health information (ePHI). Because it is an overview of the Security Rule, it does not address every detail of each provision.

This summary addresses the Security Rule that is currently in effect. Learn about OCR's Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information at HIPAA Security Rule NPRM </hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html>.

Introduction

The Security Rule establishes a national set of security standards to protect certain health information that is maintained or transmitted in electronic form. The Security Rule sets forth the administrative, physical, and technical safeguards that covered entities[4] and

business associates[5] (collectively, “regulated entities”) must put in place to secure individuals’ electronic protected health information.[6]

The Security Rule complements the privacy standards established in the Standards for Privacy of Individually Identifiable Health Information[7] under HIPAA, commonly known as the Privacy Rule;[8] and the requirements of the Breach Notification Rule, which implements provisions of the HITECH Act that direct covered entities to notify individuals, the Secretary of Health and Human Services (“HHS”), and in some cases, the media when certain information has been acquired, accessed, used or disclosed in a manner not permitted by the Privacy Rule.[9] Together, the Privacy, Security, and Breach Notification Rules help to protect the privacy and security of protected health information (PHI).[10]

A major goal of the Security Rule is to protect the security of individuals’ ePHI while allowing regulated entities to adopt new technologies that improve the quality and efficiency of health care. Because the health care marketplace is diverse, the Security Rule is designed to be flexible, scalable, and technology neutral, enabling a regulated entity to implement policies, procedures, and technologies that are appropriate for the entity’s particular size, organizational structure, and risks to ePHI.

This summary is not a comprehensive guide to compliance with the Security Rule. Regulated entities must comply with all of the applicable requirements of the Security Rule and should not rely on this summary as a source of legal information or advice. Visit our Security Rule <https://www.hhs.gov/hipaa/for-professionals/security/index.html> section to view the entire Security Rule and for additional information about how the Security Rule applies to regulated entities. In the event of a conflict between this summary and the Security Rule, the Security Rule governs.

The text of the Security Rule can be found at 45 CFR Part 160 <https://www.ecfr.gov/current/title-45/subtitle-a/subchapter-c/part-160> and Part 164 <https://www.ecfr.gov/current/title-45/subtitle-a/subchapter-c/part-164>, Subparts A and C.

Statutory and Regulatory Background

HIPAA and the Security Rule

The Administrative Simplification provisions of HIPAA requires the Secretary of HHS to adopt standards to ensure that covered entities maintain reasonable and appropriate administrative, physical, and technical safeguards for the security of certain individually

identifiable health information.[11] The statute requires that the standards do the following:

- Ensure the integrity and confidentiality of the information.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information.
- Ensure compliance with the Administrative Simplification provisions of HIPAA by the officers and employees of covered entities.[12]

HHS developed a proposed rule that included standards for protecting the confidentiality, integrity, and availability of ePHI and released it for public comment on August 12, 1998.[13] The Department received approximately 2,350 public comments. The final regulation, Standards for Privacy of Individually Identifiable Health Information (commonly known as the Security Rule), was published February 20, 2003.[14] At this time, the Security Rule only applied directly to covered entities, requiring that they implement a series of administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

The HITECH Act and Modifications to the Security Rule

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, (ARRA) contains provisions that strengthen the privacy and security protections for certain health information established under HIPAA.[15]

Section 13401 of the HITECH Act provides that the administrative, physical, and technical safeguards of the Security Rule,[16] as well as its policies and procedures and documentation requirements,[17] apply to business associates in the same manner that they apply to covered entities. It also provides that business associates are civilly and criminally liable for penalties for violations of these provisions. The 2003 Security Rule already indirectly applied to business associates because it required covered entities to enter into contracts or other written arrangements (collectively, “business associate agreements”) with business associates to ensure the confidentiality, integrity, and availability of ePHI. However, the HITECH Act provides the Department with the ability to take direct enforcement action against business associates for violating the Security Rule. Learn about the direct liability of business associates </hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>.

The Department proposed modifications to the Security Rule to implement provisions of the HITECH Act on July 14, 2010.[18] After considering public comment on the proposed rule, the Department finalized changes to the Security Rule as part of the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act Final Rule published on January 25, 2013 (commonly known as the 2013 Omnibus Final Rule).[19]

Who is Covered by the Security Rule

The Security Rule applies to:

- All of following covered entities:
  - Health plans
  - Health care clearinghouses
  - Any health care provider that transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA.[20]
- Business associates of covered entities.[21]

For help determining whether you are a covered entity, use CMS's decision tool. - PDF <https://www.cms.gov/regulations-and-guidance/administrative-simplification/hipaa-aca/downloads/coveredentitieschart20160617.pdf> Learn more about business associates </hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>.

What Information is Protected

The Security Rule protects a subset of individually identifiable health information,[22] referred to as **electronic protected health information** (ePHI),[23] which is protected health information[24] that is maintained in or transmitted by electronic media.[25] Unlike the Privacy and Breach Notification Rules, the Security Rule does not apply to PHI that is maintained or transmitted on paper or verbally.

General Rules

The Security Rule requires regulated entities to implement reasonable and appropriate administrative, physical, and technical safeguards for protecting ePHI.

Specifically, regulated entities must do all the following do all of the following:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.
2. Protect against reasonably anticipated threats to the security or integrity of the information.
3. Protect against reasonably anticipated, impermissible uses or disclosures.
4. Ensure compliance by their workforce.[26]

The Security Rule defines “confidentiality” to mean that data or information is not made available or disclosed to unauthorized persons or processes.[27] The confidentiality requirements of the Security Rule support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.[28] The Security Rule also promotes the two objectives of maintaining the integrity and availability of ePHI. Under the Security Rule, “integrity” means that data or information has not been altered or destroyed in an unauthorized manner.[29] “Availability” means that data or information is accessible and usable on demand by an authorized person.[30]

Regulated entities range in size and type, from the smallest provider to the largest, multi-state health plan, and from a medical transcriptionist to a large cloud service provider. Therefore, the Security Rule was designed to be scalable, and technology neutral to all different sizes of regulated entities.[31] This provides regulated entities with flexibility to choose security measures that are reasonable and appropriate for their size, resources, and the nature of the security risks they face.[32]

Accordingly, the Security Rule does not dictate the specific security measures that a regulated entity must use. Instead, it requires the regulated entity to consider the following factors when selecting security measures that meet the Security Rule’s requirements:

1. Its size, complexity, and capabilities.
2. Its technical infrastructure, hardware, and software security capabilities.

3. The costs of security measures.
4. The probability and criticality of potential risks to ePHI.[33]

A regulated entity must review and modify its security measures to continue reasonable and appropriate protection of ePHI, and update documentation of its security measures.[34]

Risk Analysis and Management

The Administrative Safeguards provisions in the Security Rule require a regulated entity to perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the regulated entity as part of their security management processes. The risk analysis and risk management provisions of the Security Rule are addressed separately here because a risk analysis affects the implementation of all of the safeguards contained in the Security Rule by helping a regulated entity to identify potential risks and vulnerabilities. Based on the potential risks and vulnerabilities the regulated entity identifies, it then determines which security measures are reasonable and appropriate to implement for managing that risk.

A regulated entity must implement procedures to regularly review its records to track access to ePHI and detect security incidents,[35] periodically evaluate the effectiveness of security measures put in place and modify such security measures as necessary,[36] and regularly reevaluate potential risks to ePHI.[37]

To assist regulated entities, OCR has issued guidance on conducting a risk assessment.

Administrative Safeguards

- **Security Management Process.** A regulated entity must perform an accurate and thorough assessment of potential risks and vulnerabilities to ePHI,[38] and it must manage risks by implementing security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.[39]
- **Assigned Security Responsibility.** A regulated entity must designate a security official responsible for developing and implementing the policies and procedures required by the Security Rule.[40]

- **Workforce Security.** A regulated entity must implement policies and procedures to ensure that workforce members who work with ePHI have appropriate authorization, supervision, and access to ePHI.[41]
- **Information Access Management.** Consistent with the Privacy Rule's "minimum necessary" standard limiting uses and disclosures of PHI,[42] the Security Rule requires a regulated entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate for the user or recipient's role.[43]
- **Security Awareness and Training.** A regulated entity must train all workforce members on its security policies and procedures.[44] Additionally, a regulated entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures.[45]
- **Security Incident Procedures.** A regulated entity must implement policies and procedures to address security incidents. It must identify and respond to suspected or known security incidents and mitigate, to the extent possible, harmful effects of known security incidents, and document security incidents and their outcomes.[46]
- **Contingency Plan.** A regulated entity must establish and implement procedures for responding to emergencies or other occurrences that damage information systems that contain ePHI.[47] This includes establishing plans for backing up its ePHI, restoring any lost data, and continuing critical business processes for protecting the security of ePHI while operating in emergency mode.[48]
- **Evaluation.** A regulated entity must perform a periodic technical and non-technical assessment of how well its policies and procedures meet the requirements of the Security Rule.[49] As part of the assessment, regulated entities must periodically evaluate their security safeguards to demonstrate and document their compliance with their security policy and the Security Rule.[50] They must assess the need for a new evaluation based on the changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their ePHI.[51]
- **Business Associate Contracts and Other Arrangements.** Before permitting a business associate to create, receive, maintain, or transmit ePHI, a regulated entity must have in place a contract or other written arrangement (collectively referred to as a “business associate agreement”) that complies with the requirements described below in the section on Organizational Requirements.[52]

Physical Safeguards

- **Facility Access and Control.** A regulated entity must implement policies and procedures to limit physical access to its electronic information systems and facilities that house such systems while ensuring that properly authorized access is allowed.[53]
- **Workstation Use and Security.** A regulated entity must implement policies and procedures to specify proper use of, and physical safeguards for, workstations that can access ePHI.[54]
- **Device and Media Controls.** A regulated entity must have in place policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility, including the final disposition of ePHI and the hardware or electronic media on which it is stored.[55] The regulated entity must also implement procedures for removing ePHI from electronic media before the media are made available for re-use.[56]

Technical Safeguards

- **Access Control.** A regulated entity must implement technical policies and procedures for its electronic information systems that maintain ePHI to allow only authorized persons to access ePHI.[57]
- **Audit Controls.** A regulated entity must implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI.[58]
- A regulated entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that ePHI has not been improperly altered or destroyed.[59]
- **Authentication.** A regulated entity must implement procedures to verify that a person seeking access to ePHI is who they say they are.[60]
- **Transmission Security.** A regulated entity must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic network.[61]

Required and Addressable Implementation Specifications

Regulated entities are required to comply with every Security Rule "standard." However, some of the flexibility and scalability afforded by the Security Rule to regulated entities is achieved by categorizing certain implementation specifications within those standards as "addressable" and others as "required."

The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. Rather, it permits regulated entities to determine whether the addressable implementation specification is reasonable and appropriate for that regulated entity. Where it is reasonable and appropriate, the regulated entity must adopt the addressable implementation specification. Where an addressable implementation specification it is not reasonable and appropriate, the Security Rule allows the regulated entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.[62] In such cases, the regulated entity must also document why it is not reasonable and appropriate to implement the addressable implementation specification.[63]

Organizational Requirements

Business Associate Contracts or Other Arrangements. Regulated entities are required to enter into written contracts or other arrangements referred to as “business associate agreements.”[64]

Under the Security Rule, a covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on its behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.[65]

The business associate agreement must do the following:

- Document the required satisfactory assurances.[66]
- Provide that the business associate will comply with the Security Rule.[67]

- Commit the business associate to ensuring that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the Security Rule by entering into a business associate agreement with the subcontractor.[68]
- Obligate the business associate to report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI as required by the Breach Notification Rule.[69]

Business Associate Responsibilities. The Security Rule does not require a covered entity to obtain satisfactory assurances from a business associate that is a subcontractor.[70] However, a business associate is required to obtain satisfactory assurances in the form of a contract or other written agreement from a subcontractor that creates, receives, maintains, or transmits ePHI on its behalf.[71] Such agreements must meet the same requirements as those for a business associate agreement between a covered entity and a business associate.[72]

Policies and Procedures and Documentation Requirements

- **Policies and Procedures.** A regulated entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule.[73]
- **Documentation.** A regulated entity must maintain documentation required for written policies and procedures implemented to comply with the Security Rule and actions, activities, or assessments required by the Security Rule to be documented until six years after the later of: 1) the date of the document's creation or 2) the date the document was last in effect.[74]
- **Availability.** A regulated entity must make the written policies and procedures it implements to comply with the Security Rule and its documentation of required actions, activities, and assessments available to those persons responsible for implementing the procedures described in the documentation.[75]
- **Updates.** A regulated entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.[76]

Endnotes

[1]Subtitle F of title II of HIPAA (Pub. L. 104–191, 110 Stat. 1936 (Aug. 21, 1996)).

[2] 45 CFR part 160 and subparts A and C of part 164.

[3] Pub. L. 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 139w–4(0)(2)).

[4] *See* 45 CFR 160.103 (definition of "Covered entity").

[5] *See* 45 CFR 160.103 (definition of "Business associate").

[6] *See* 45 CFR 160.103 (definition of "Electronic protected health information").

[7] *See* 45 CFR 160.103 (definition of "Individually identifiable health information").

[8] 45 CFR part 160 and subparts A and E of part 164.

[9] 45 CFR part 160 and subparts A and D of part 164. Under the Breach Notification Rule, a business associate is required to provide such notification to a covered entity. *See* 45 CFR 164.410.

[10] *See* 45 CFR 160.103 (definition of "Protected health information").

[11] *See* 42 U.S.C. 1173(d)(2).

[12] *Id.*

[13]*See generally* 63 FR 43242 (Aug. 12,1998).

[14] *See* 68 FR 8334 (Feb. 20, 2003).

[15] *See* subtitle D of Title XIII of Division A of ARRA, Pub. L. 111-5, 123 Stat. 115 (Feb. 1, 2009) (codified at 42 U.S.C. 201 note).

[16] *See* 45 CFR 164.308, 164.310, and 164.312.

[17] *See* 45 CFR 164.316.

[18] *See* 75 FR 40868 (July 14, 2010).

[19] *See* 78 FR 5566 (Jan. 25, 2013).

[20] *See* 45 CFR 160.103 (definition of "Covered entity").

[21] *See* 45 CFR 160.103 (definition of “Business associate”).

[22] *See* 45 CFR 160.103 (definition of “Individually identifiable health information”).

[23] *See* 45 CFR 160.103 (definition of “Electronic protected health information”).

[24] *See* 45 CFR 160.103 (definition of “Protected health information”).

[25] *See* 45 CFR 160.103 (definition of “Electronic media”).

[26] *See* 45 CFR 164.306(a).

[27] *See* 45 CFR 164.304 (definition of “Confidentiality”).

[28] *See generally* 45 CFR part 160 and subparts A and E of part 164.

[29] *See* 45 CFR 164.304 (definition of “Integrity”).

[30] *See* 45 CFR 164.304 (definition of “Availability”).

[31] *See* 78 FR 5565, 5589 (Jan. 25, 2013).

[32] *Id*

[33] *See* 45 CFR 164.306(b)(2).

[34] *See* 45 CFR 164.306(e).

[35] *See* 45 CFR 164.308(a)(1)(ii)(D).

[36] *See* 45 CFR 164.306(e); 45 CFR 164.308(a)(8).

[37] *See* 45 CFR 164.306(b)(2)(iv); 45 CFR 164.306(e).

[38] *See* 45 CFR 164.308(a)(1)(ii)(A).

[39] *See* 45 CFR 164.308(a)(1)(ii)(B).

[40] *See* 45 CFR 164.308(a)(2).

[41] *See* 45 CFR 164.308(a)(3) and (4).

[42] *See* 45 CFR 164.514(d).

[43] *See* 45 CFR 164.308(a)(4)(i).

[44] *See* 45 CFR 164.308(a)(5)(i).

[45] *See* 45 CFR 164.308(a)(1)(ii)(C).

[46] *See* 45 CFR 164.308(a)(6).

[47] *See* 45 CFR 164.308(a)(7)(i).

[48] *See* 45 CFR 164.308(a)(7)(ii).

[49] *See* 45 CFR 164.308(a)(8).

[50] *See* 68 FR 8334, 8351 (Feb. 20, 2003).

[51] *Id.*

[52] *See* 45 CFR 164.308(b).

[53] *See* 45 CFR 164.310(a).

[54] *See* 45 CFR 164.310(b) and (c).

[55] *See* 45 CFR 164.310(d).

[56] *See* 45 CFR 164.310(d)(ii).

[57] *See* 45 CFR 164.312(a).

[58] *See* 45 CFR 164.312(b).

[59] *See* 45 CFR 164.312(c).

[60] *See* 45 CFR 164.312(d).

[61] *See* 45 CFR 164.312(e).

[62] *See* 45 CFR 164.306(d).

[63] *See* 45 CFR 164.306(d)(1)(ii)(B)(*1*).

[64] *See* 45 CFR 164.308(b)(3).

[65] *See* 45 CFR 164.308(b)(1).

[66] *See* 45 CFR 164.308(b)(3).

[67] *See* 45 CFR 164.314(a)(2)(i)(A).

[68] *See* 45 CFR 164.314(a)(2)(i)(B).

[69] *See* 45 CFR 164.314(a)(2)(C); 45 CFR part 160 and subparts A and D of subpart 164.

[70] *See* 45 CFR 164.308(b)(1).

[71] *See* 45 CFR 164.308(b)(2).

[72] *See* 45 CFR 164.314(a)(2)(iii).

[73] *See* 45 CFR 164.316(a).

[74] *See* 45 CFR 164.316(b)(2)(i).

[75] *See* 45 CFR 164.316(b)(2)(ii).

[76] 45 CFR 164.316(b)(2)(iii).

Content created by Office for Civil Rights (OCR)
Content last reviewed December 30, 2024