From the CCH Health Care Compliance Professional's Manual

HIPAA Security Rule

CCH-EXP, Health-Comp-Manual, **¶20,811 Introduction**
Introduction

Since April 20, 2005, the same organizations that are required to comply with the HIPAA Privacy Rule must also comply with the HIPAA Security Rule. This chapter discusses HIPAA's security requirements and provides compliance officers with suggestions for developing and maintaining HIPAA security.

This chapter will refer to the collection of regulations promulgated under the authority of the Health Insurance Portability & Accountability Act of 1996 (HIPAA) that treat the security of electronic protected health information as the Security Rule.[1] We will also refer to the regulations under HIPAA that address the privacy of protected health information as the Privacy Rule.[2] This chapter assumes that the reader has a working familiarity with the Privacy Rule.

History of the Security Rule

HIPAA was passed by Congress in 1996.[3] As a result of that legislation, the United States Department of Health and Human Services (HHS) was directed to develop regulations regarding the privacy and security of health information handled and maintained by various actors in the health care industry.

HHS published proposed regulations in the Federal Register regarding the security of health information maintained or transmitted in electronic form on August 12, 1998.[4] The proposed regulations also included regulations regarding the use of electronic signatures.

The final Security Rule was published in the Federal Register on February 20, 2003 and contains only security standards and requirements.[5] A final set of regulations regarding the use of electronic signatures will be published by HHS at a later date. As of this writing, this is no indication when the final electronic signature regulations will be published.

[1] 45 C.F.R. §164.102, et seq.

[2] 45 C.F.R. §164.500, et seq.

[3] Pub. L. 104-191.

[4] 63 FR 43242.

[5] 68 FR 8334.

CCH-EXP, Health-Comp-Manual, **¶20,812 Introduction**
Introduction

Covered Entities

The Security Rule only applies to covered entities.[6] A covered entity is any health care provider that submits electronic standard transactions, health plan or health care clearinghouse.[7] These are the same entities that must comply with the Privacy Rule. If an organization is not a covered entity, then it need not comply with the Security Rule.

As discussed below, the Security Rule requires covered entities to obligate their business associates through written agreements to implement security measures.[8] The Security Rule added a few provisions to the list of provisions that the Privacy Rule already required in a business associate agreement.

Electronic Protected Health Information

The Security Rule only regulates measures that safeguard electronic protected health information.[9] This is contrasted with the Privacy Rule, which regulates all forms of protected health information, whether in electronic, written or oral form.[10]

Electronic protected health information is any individually identifiable health information created, received or maintained by a covered entity in electronic format. The Security Rule utilizes the same definition of individually identifiable health information as the Privacy Rule.[11]

The result of the Security Rule's applicability to only electronic protected health information is that covered entities that can easily compartmentalize electronic protected health information from electronic information that is not protected health information need not implement the Security Rule's safeguards for the information that is not protected health information. For many covered entities it will be impossible to cleanly compartmentalize operations that deal with electronic protected health information from those that involve only non-protected health information. For these organizations, it may be easier to implement the Security Rule's safeguards to protect all electronic information rather than just electronic protected health information.

Additionally, for covered entities that have no electronic protected health information (e.g., some small physician offices), they may not need to implement any of the Security Rule's requirements.

This chapter will discuss the requirements of the Security Rule in the context of safeguarding electronic protected health information, but every covered entity that is deciding how to comply with the Security Rule should consider whether a specification of the Security Rule should be expanded to protect all electronic information for practical ease in compliance.

[6] 45 C.F.R. §164.306.

[7] 45 C.F.R. §160.103.

[8] 45 C.F.R. §164.308(b).

[9] 45 C.F.R. §164.306(a)(1).

[10] 45 C.F.R. §164.500(a).

[11] 45 C.F.R. §160.103.

CCH-EXP, Health-Comp-Manual, **¶20,813 Structure of the Security Rule**

Structure of the Security Rule

Unlike many health care regulations, the Security Rule is highly organized and understanding the structure of the Security Rule is critical to effective compliance with it. The Security Rule sets out its obligations in categories of "safeguards," "standards," and "implementation specifications." The specifications are divided between "required implementation specifications" and "addressable implementation specifications."

Safeguards

The Security Rule sets out three broad categories of safeguards: administrative safeguards, physical safeguards and technical safeguards. All standards and specifications fall under one of these three safeguards.[12] Some aspects of implementation specifications are discussed in multiple safeguard categories but the relevant aspect of the specification (administrative, physical or technical) is discussed under the respective safeguard. This chapter deals with specifications under each of the safeguards as they are set out in the Security Rule.

Standards

A covered entity must comply with all standards set out under each of the three safeguards.[13] For standards that have implementation specifications, the standard often serves as the policy goal of the specifications and provides insight into how to implement the specifications. The standards play particular importance in implementing addressable specifications and justifying alternative measures allowed under an addressable specification.

Required & Addressable Implementation Specifications

Most of the Security Rule's standards set out implementation specifications that are designated as either required or addressable specifications. The implementation specifications provide the detail on how a covered entity will meet the various standards. When an implementation specification is a required specification, then the covered entity must comply with the implementation specification as the specification is written.[14] When an implementation specification is an addressable specification, then the covered entity must implement the specification as written if it reasonable and appropriate to implement the specification. If it is not reasonable and appropriate to implement the specification as it is written, then the covered entity must 1) document why it is not reasonable and appropriate to implement the specification, and 2) determine whether there is an alternative measure that can be implemented that satisfies the goal of the specification and the standard that the specification supports. If there are no alternative measures that are reasonable or appropriate to implement, the covered entity need not comply with the addressable specification. [15]

For consideration of how to determine whether an approach is reasonable and appropriate, please see the discussion below on the Security Rule's flexibility approach.

The Security Rule sets out a process for determining whether an addressable implementation specification must be complied with as written or whether alternative measures can be employed. Below is a process that closely follows the Security Rule's considerations for addressable implementation specifications:

1. Is the addressable implementation specification applicable to the covered entity?
   - If not, then the covered entity need not comply with the implementation specification.

2. Is it reasonable and appropriate for the covered entity to implement the measures described in the addressable implementation specification?
   - If it is reasonable and appropriate, then the covered entity must implement the addressable implementation specification as it is written.

   - If it is not reasonable or appropriate to implement the measures in the addressable implementation specification, then the covered entity should consider whether there are any alternative measures that are reasonable and appropriate.

3. Is there an equivalent alternative measure that can be implemented that meets the goals of the implementation specification and the specification's standard?

- If the alternative measure is reasonable and appropriate, then the covered entity must implement that alternative measure.

- If there is no alternative measure that is reasonable or appropriate for the covered entity to implement, then the covered entity need not comply with the addressable implementation specification.

All parts of the implementation process of an addressable specification that does not implement the specification as written, must be thoroughly documented. In the above questions, the following should be documented: why an addressable implementation specification is not applicable to a covered entity; why the addressable specification cannot be implement as written; why an alternative measure is reasonable, appropriate and meets the goals of the implementation specification and the specification's standards; why no alternative measure exists that is reasonable or appropriate.

The addressable implementation specifications are sometimes characterized as optional, as if there is a choice whether to implement them or not. This is an erroneous characterization of addressable implementation specifications. Addressable implementation specifications must be complied with, but unlike required implementation specifications, the way the addressable implementation specification is complied with can take many forms based on the considerations discussed above. Only under the most dire conditions may an addressable implementation specification be dispensed with and only when no alternative measure can be reasonably implemented. A covered entity should be vigilant of any addressable implementation specification it decides that it will not comply with. The circumstances of what is reasonable can change quickly. If the measures or alternative measures of the addressable implementation specification become reasonable and appropriate, then the covered entity must comply with the specification.

Also, a covered entity that determines it need not implement a particular addressable implementation specification should, to the extent possible, monitor what industry standards are for other similarly situated covered entities are doing regarding the implementation specification. It will be very difficult for a covered entity to justify the position that it is not reasonable and appropriate to implement an implementation specification if most other similarly situated covered entities have implemented the specification as written in the Security Rule.

Flexibility Approach

One of the hallmarks of the Security Rule is its "flexibility approach." While the Security Rule's standards and specifications provide a considerable amount of detail for implementation, there are innumerable ways to implement the requirements and there are many specifications that are left up to the covered entity to fill in the detail. For instance, the Security Rule requires automatic log-offs but the Security Rule does not tell a covered entity what length of inactivity should trigger the automatic log-off. Should automatic log-offs be triggered at 30 minutes, 15 minutes, 5 minutes or 1 minute? Or, do different circumstances necessitate different log-off times? The Security Rule's flexibility approach allows a covered entity to judge for itself how these details should be filled in, as long as the covered entity's approach is reasonable and appropriate given the level of risk.

The Security Rule states that "covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this [Rule]."[16] In determining what is reasonable and appropriate, the Security Rule requires covered entities to consider the following:[17]

1. The size, complexity, and capabilities of the covered entity.
2. The covered entity's technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

The goals of the Security Rule provide an important framework for interpreting and complying with the Security Rule. At various points in the implementation specifications, the goals are explicitly referenced. Even when they are not explicitly referenced, it is important to keep the Security Rule's goals in mind when determining what security measures may be reasonable or appropriate.

Consequently, all measures that a covered entity implements to comply with the standards and specifications of the Security Rule must accomplish the following:[18]

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of a covered entity's electronic protected information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and
4. Ensure compliance with the Security Rule by a covered entity's workforce.

[12] 45 C.F.R. §§164.308, 164.310, 164.312.

[13] 45 C.F.R. §164.306(c).

[14] 45 C.F.R. §164.306(d)(2).

[15] 45 C.F.R. §164.306(d)(3).

[16] 45 C.F.R. §164.306(b)(1).

[17] 45 C.F.R. §164.306(b)(2).

[18] 45 C.F.R. §164.306(a).

CCH-EXP, Health-Comp-Manual, **¶20,814 Introduction**
Introduction

The Security Rule's administrative safeguards address many of the institutional structures of ensuring the security and integrity of electronic protected health information. Many of the administrative safeguards provide the backbone of a HIPAA Security Compliance Program. There is no one, right way to develop a HIPAA Security Compliance Program. In fact, the term "compliance program" is not used in either the Security Rule or the Privacy Rule, but the administrative requirements of both of these rules contain many of the properties of the seven basic elements of an effective compliance program.

It makes practical sense to think of a HIPAA Security Compliance Program in the same light as other compliance programs. Many covered entities incorporate their security compliance measures into an existing corporate compliance program. In many cases, an organization may not choose the Chief Compliance Officer to be the Security Official, but the organizational structure for the security compliance initiative and the auditing and monitoring of security compliance will be located in the same organization structure that maintains the corporate compliance program.

CCH-EXP, Health-Comp-Manual, **¶20,815 Security Management Process**
Security Management Process

The Security Management Process Standard has four required specifications on implementing the Security Rule's mandate that covered entities "Implement policies and procedures to prevent, detect, contain, and correct security violations."[19]

Risk Analysis

The first implementation specification that supports this standard requires a covered entity to "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."[20]

This specification is generally considered to require all covered entities to perform a risk assessment of all operations that deal with electronic protected health information. It is important to keep in mind that this risk analysis must be done with respect to all three safeguards - administrative, physical and technical - and whether the current measures the covered entity employs is sufficient to meet the standards and goals of the Security Rule. Because the physical safeguards are considered just as important as the administrative and technical safeguards, a covered entity's risk assessment should review all locations of a covered entity that deal with electronic protected health information.

How a risk assessment is conducted can vary by covered entity. There is no mandatory format that the risk assessment should take. A common approach is to utilize the standards and specifications of the Security Rule and simply assess how each location of the covered entity attempts to accomplish the standards now and determine what it will take for the covered entity to implement the standards and specifications that the covered entity currently is not complying with. The risk analysis should be documented.

There is no requirement in this specification that the covered entity repeat its risk assessment, though the Security Rule elsewhere requires covered entities to review and modify the security measures it implements. In order to demonstrate an effective HIPAA Security Compliance Program, a covered entity should have an active and dynamic auditing and monitoring plan. From a Security Rule perspective, regular risk assessments would likely be viewed as a critical dimension to any security auditing and monitoring plan.

Risk Management

A covered entity must "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the goals of the Security Rule]."[21] This implementation specification references the same goals that are discussed above in ¶20,813.

CMS has issued guidance on the difference between risk management and risk analysis. In an FAQ dated August 8, 2004, CMS first sets out its understanding of risk analysis as "the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic PHI held by a covered entity, and the likelihood of occurrence."[22] CMS then contrasts this with its understanding of risk management as "the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its electronic PHI and to meet the general security standards."[23]

Consequently, risk management can be seen as the approach a covered entity takes to minimize the risks identified in the risk analysis. A covered entity should document thoroughly the measures it implements to manage its security risks.

Sanction Policy

A covered entity must "apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."[24]

It is important that a covered entity's sanctions policy apply to all workforce members equally. A covered entity should also consider whether its existing compliance sanctions policy would cover violations of its security policies and procedures. If the current compliance sanctions policy would not cover security policy violations, then a covered entity should consider incorporating language into the general compliance sanctions policy for ease in applying a consistent sanctions approach.

Information System Activity Review

A covered entity must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[25]

This specification speaks to the need to develop a security auditing and monitoring plan. The specification does not provide what frequency these regular reviews should be done, but covered entities should consider performing security reviews and audits at least once per year. Many covered entities are spreading out their reviews and audits over the course of a year and performing portions of these reviews on a quarterly basis.

[19] 45 C.F.R. §164.308(a)(1)(i).

[20] 45 C.F.R. §164.308(a)(1)(ii)(A).

[21] 45 C.F.R. §164.308(a)(1)(ii)(B).

[22] CMS FAQ Answer ID3228.

[23] *Id.*

[24] 45 C.F.R. §164.308(a)(1)(ii)(C).

[25] 45 C.F.R. §164.308(a)(1)(ii)(D).

CCH-EXP, Health-Comp-Manual, **¶20,816 Assigned Security Responsibility**
Assigned Security Responsibility

The Assigned Security Responsibility Standard requires that a covered entity "identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."[26] Since this standard has no implementation specification, a covered entity is required to implement this standard as it is written.

This required standard deals with the Security Official of the covered entity. A Security Official (also sometimes called the Security Officer) is the person who must spearhead, organize and maintain the covered entity's HIPAA Security Compliance Program.

The Security Rule does not speak to what qualifications the Security Official should have or to whom the Security Official should report. Many covered entities appoint their chief information officer (CIO) as the Security Official. For some organizations, the CIO may be the right person for the job, but for other organizations the CIO may not be the right person if the CIO does not have a broad understanding of the operations of the covered entity. The Security Official should, most importantly, have a good understanding of what the covered entity does and how the covered entity is organized in order to deliver its services. Having a technology background and understanding can be helpful to the Security Official but is not required as long as the Security Official can rely on the CIO for technical help and support.

[26] 45 C.F.R. §164.308(a)(2).

CCH-EXP, Health-Comp-Manual, **¶20,817 Workforce Security**

Workforce Security

The Workforce Security Standard has three implementation specifications that detail what a covered entity must do to "implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management Standard section of the Security Rule] of this section, and to prevent those workforce members who do not have access under that section from obtaining access to electronic protected health information."[27] The Information Access Management Standard section of the Security Rule is discussed below in ¶20,818 of this chapter.

Authorization and/or Supervision

A covered entity should "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."[28]

This specification requires a covered entity to devise some process whereby the workforce member's access rights are reviewed prior to receiving such rights. Many organizations are centralizing the authorization process so that a manager or supervisor recommends access authorization to the information technology department and someone in the information technology department enables the workforce member's user identification and access to the information systems.

Workforce Clearance Procedure

A covered entity should "implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."[29]

Covered entities approach workforce clearance in a variety of ways. One approach is to clearly state in the covered entity's policies that an information system user will not be granted access to the covered entity's information systems until after the individual has cleared the organization's normal compliance clearance process.

Termination Procedures

A covered entity should "implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in [the workforce clearance procedures].”[30]

It is important that when a workforce member is no longer associated with the covered entity, the individual’s access to the information systems be terminated as quickly as possible. Termination procedures may differ for instances in which the individual has voluntarily left as opposed to instances where the individual was involuntarily terminated.

In covered entities in which the human resources department coordinates departures from the organization, this specification may be able to be met by the human resources department immediately contacting the information technology department to inform them of a departure. The information technology department should terminate the person’s access to electronic protected health information pursuant to termination policies and procedures. Covered entities must also implement procedures for when business associates who have access to information systems are no longer providing services to the organization.

[27] 45 C.F.R. §164.308(a)(3)(i).

[28] 45 C.F.R. §164.308(a)(3)(ii)(A).

[29] 45 C.F.R. §164.308(a)(3)(ii)(B).

[30] 45 C.F.R. §164.308(a)(3)(ii)(C).

CCH-EXP, Health-Comp-Manual, **¶20,818 Information Access Management**
Information Access Management

The Information Access Management Standard has three implementation specifications that detail what a covered entity must do to “implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of [the Privacy Rule].”[31]

Isolating Health Care Clearinghouse Function

A covered entity must examine its operations to determine if it performs any health care clearinghouse functions. “If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the [other parts of the organization].”[32]

Access Authorization

A covered entity should “implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.”[33]

Access Establishment and Modification

A covered entity should “implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.”[34]

[31] 45 C.F.R. §164.308(a)(4)(i).

[32] 45 C.F.R. §164.308(a)(4)(ii)(A).

[33] 45 C.F.R. §164.308(a)(4)(ii)(B).

[34] 45 C.F.R. §164.308(a)(4)(ii)(C).

CCH-EXP, Health-Comp-Manual, **¶20,819 Security Awareness and Training**
Security Awareness and Training

The Security Awareness and Training Standard has four implementation specifications that detail how a covered entity should "implement a security awareness and training program for all members of its workforce (including management)."[35]

Security Reminders

A covered entity should issue "periodic security updates."[36] Covered entities should regularly issue reminders and explanations of the organization's security policies and procedures. For instance, on a quarterly basis the Security Official could issue a newsletter or send emails that highlight a particular aspect of the security policies and procedures (e.g., reminding the workforce not to share passwords).

Protection from Malicious Software

A covered entity should implement measures that provide "protection from malicious software" that involve "procedures for guarding against, detecting, and reporting malicious software."[37]

Log-in Monitoring

A covered entity should implement "procedures for monitoring log-in attempts and reporting discrepancies."[38] This specification does not discuss how many log-in failures a covered entity should allow before disabling a user identification. Log-in failure limits between three and five appear to be common. A covered entity may choose to use different limits based on the applications or electronic protected health information that the user is authorized to access. For instance, a user with access to particularly sensitive information may have a lower limit than a user with access to only more general information.

Password Management

A covered entity should implement "procedures for creating, changing, and safeguarding passwords."[39] This specification does not discuss how passwords should be generated or how frequently passwords should be changed. It is common for organizations to warn users not to choose passwords that other people could easily figure out (e.g., mother's maiden name; children names; etc.). With respect to frequency for changing passwords, 90 days is a common time frame. If an information system has the capability to force passwords to be changed on a regular basis, then a covered entity would be wise to enable such a feature.

Similarly, the Security Rule does not provide guidance as to how robust passwords should be. Some information security specialists suggest that all passwords should contain a combination of numbers and letters, at least one capitalized letter, and at least one special character. Of course, a balance must be struck between having passwords that are secure from detection by malware that is designed to guess a person's password and passwords that are so complex that individuals cannot remember them.

[35] 45 C.F.R. §164.308(a)(5)(i).

[36] 45 C.F.R. §164.308(a)(5)(ii)(A).

[37] 45 C.F.R. §164.308(a)(5)(ii)(B).

[38] 45 C.F.R. §164.308(a)(5)(ii)(C).

[39] 45 C.F.R. §164.308(a)(5)(ii)(D).

CCH-EXP, Health-Comp-Manual, **¶20,820 Security Incident Procedures**
Security Incident Procedures

The Security Incident Procedures Standard has one required implementation specification that provides detail on how a covered entity should implement "policies and procedures to address security incidents."[40]

The definition of "security incident" is one of the most controversial aspects of the Security Rule. The Security Rule sets out the definition of "security incident" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." Importantly, this definition includes both successful and attempted unauthorized access, use, etc. Pings on a firewall that are successively repelled, and viruses that are detected and blocked by an organization's security measures are but two examples of security incidents as defined in the Security Rule. For many information systems, these kinds of events occur tens of thousands of times per day. There was some discussion within the health care industry on whether this definition may be revised to include only successful incidents. On May 4, 2005, CMS issued an FAQ on security incidents that appears to put to rest any speculation that the definition will be changed in the near future.[41] Both successful and unsuccessful unauthorized access, etc. remain in the definition of a security incident, and covered entities must determine how to comply with this standard and its required implementation specification under this definition.

Response and Reporting

A covered entity must "identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."[42] The CMS FAQ from May 2005 states that "in order to maintain a flexible, scalable and technology neutral approach to the Security Rule, no single method is identified for addressing security incidents that will apply to all covered entities."[43]

Many organizations are designing approaches that deal with successful incidents differently from attempted incidents in order to make dealing with the attempted incidents more manageable. For instance, some organizations require every known successful incident to be investigated, whereas for attempted incidents the organizations require that they be tracked, but rather than investigate every attempted incident, the covered entity examines patterns and trends in order to identify weaknesses, vulnerabilities and to identify the source of the attempts. The CMS FAQ appears to support innovative ways to both comply with the specification and make management of security incidents reasonable. The FAQ states that it is appropriate for a covered entity to determine "whether identifying patterns of attempted security incidents is reasonable and appropriate."[44] The FAQ further states that "the covered entity may decide that certain types of attempted or successful incidents warrant different actions."[45]

Many organizations will categorize security incidents by the threat that the incident poses to electronic protected health information and develop response procedures that are specific for each category. Covered entities will need to determine who will be involved in the initial response and investigation, whether or not individuals whose information may have been compromised will be informed, and whether any governmental agencies (such as law enforcement and regulatory agencies) need to be informed of the incident based on the category in which the incident falls.

[40] 45 C.F.R. §164.308(a)(6).

[41] CMS FAQ Answer ID4734.

[42] 45 C.F.R. §164.308(a)(6)(ii).

[43] CMS FAQ Answer ID4734.

[44] *Id.*

[45] *Id.*

CCH-EXP, Health-Comp-Manual, **¶20,821 Contingency Plan**
Contingency Plan

The Contingency Plan Standard has five implementation specifications that set out the details for how a covered entity should "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."[46]

A covered entity should consider whether some of the contingency plan specifications mirror current activities that the organization may be undertaking as part of its disaster planning.

Data Backup Plan

A covered entity must "implement procedures to create and maintain retrievable exact copies of electronic protected health information".[47]

Disaster Recovery Plan

A covered entity must "establish (and implement as needed) procedures to restore any loss of data."[48]

Emergency Mode Operation Plan

A covered entity should "establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."[49]

Testing and Revision Procedure

A covered entity should "implement procedures for periodic testing and revision of contingency plans."[50] This specification does not state how frequently the periodic testing should occur, but many organizations perform testing at a minimum annually.

Applications and Data Criticality Analysis

A covered entity should "assess the relative criticality of specific applications and data in support of other contingency plan components."[51]

[46] 45 C.F.R. §164.308(a)(7)(i).

[47] 45 C.F.R. §164.308(a)(7)(ii)(A).

[48] 45 C.F.R. §164.308(a)(7)(ii)(B).

[49] 45 C.F.R. §164.308(a)(7)(ii)(C).

[50] 45 C.F.R. §164.308(a)(7)(ii)(D).

[51] 45 C.F.R. §164.308(a)(7)(ii)(E).

CCH-EXP, Health-Comp-Manual, **¶20,822 Evaluation**
Evaluation

The Evaluation Standard requires a covered entity to "perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under [the Security Rule] and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule]."[52] This standard has no implementation specifications and therefore the standard must be implemented as written. Likewise, the Security Rule does not specify how often the evaluation should be performed. Many covered entities are planning on performing an evaluation annually and whenever, in the judgment of the Security Official, environmental or operational changes call for an interim evaluation.

[52] 45 C.F.R. §164.308(a)(8).

CCH-EXP, Health-Comp-Manual, **¶20,823 Business Associate Contracts and Other Arrangements**
Business Associate Contracts and Other Arrangements

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 from the business associate "satisfactory assurances" that the business associate will appropriately safeguard the information.[53]

This requirement does not apply to situations where:[54]

1) the covered entity transmits electronic protected health information to a healthcare provider concerning the treatment of an individual;

2) a group health plan, or an HMO or a health insurance carrier on behalf of the group health plan, transmits electronic protected health information to the plan sponsor, provided that requirements regarding group health plan documents contained in the Security Rule and the Privacy Rule are satisfied;

3) a group health plan that is a government program transmits electronic protected health information to another government agency for eligibility or enrollment purposes, provided that certain Privacy Rule requirements are satisfied.

Written Contract or Other Arrangement

The "satisfactory assurances" must be documented through a written agreement between the covered entity and the business associate, or when both the covered entity and business associate our governmental agencies, a memorandum of understanding.[55]

A business associate agreement must require the business associate to:[56]

1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that the business associate creates, receives, maintains, or transmits on behalf of the covered entity;

2) ensure that any agent, including a subcontractor, to which the business associate provides such information, agrees to implement reasonable and appropriate safeguards to protect it;

3) report to the covered entity any security incident of which the business associate becomes aware; and

4) authorize termination of the agreement by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

The requirement to ensure that the business associate's agents agree to appropriate safeguards, and the requirement that the contract authorize termination by the covered entity in the event of a material breach by the business associate, were already required provisions in a business associate agreement under the Privacy Rule.

Presumably, covered entities have already identified their business associates and have put business associate agreements in place as required by the Privacy Rule. Such agreements can be amended to add the additional provisions required by the Security Rule. There is no need, from a regulatory compliance perspective, to enter into an entirely new agreement with each business associate in order to add the Security Rule language.

When a covered entity and its business associate are both governmental entities, a memorandum of understanding that contains terms that accomplish the objectives of the required provisions listed above is sufficient.[57] Such entities need not enter into a formal agreement. The covered entity may omit from the memorandum the provision authorizing termination of the arrangement by the covered entity if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

If an entity is required by law to perform a function on behalf of a covered entity that makes it a business associate, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information to the extent necessary to comply with the legal mandate without first entering into a business associate agreement or memorandum of understanding.[58] In such cases, the covered entity must attempt in good faith to get the business associate to enter into a business associate agreement or memorandum of understanding, as applicable, and document the attempt and the reasons that the appropriate arrangement could not be entered into.

[53] 45 C.F.R. §164.308(b)(1).

[54] 45 C.F.R. §164.308(b)(2).

[55] 45 C.F.R. §164.308(b)(4).

[56] 45 C.F.R. §164.314(a)(2).

[57] 45 C.F.R. §164.314(a)(2)(ii)(A).

[58] 45 C.F.R. §164.314(a)(2)(ii)(B).

CCH-EXP, Health-Comp-Manual, **¶20,824 Facility Access Controls**
Facility Access Controls

The Facility Access Controls Standard has four implementation specifications that provide detail on how a covered entity should "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."[59]

Contingency Operations

A covered entity should "establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."[60] This specification should be incorporated into the measures taken to comply with the Contingency Plan Standard for administrative safeguards.

Facility Security Plan

A covered entity should "implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."[61]

Access Control and Validation Procedures

A covered entity should "implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."[62]

This specification has also generated considerable controversy. A plain interpretation of this specification suggests that access should be controlled and validated for anyone who enters a facility that contains electronic protected health information. Some approaches that covered entities have utilized include requiring employees to wear name badges or other identification. Health care providers typically already have identification systems designed for patients. Visitor control can take the form of visitor badges or showing identification at a front desk.

One aspect of access control that is important for covered entities to consider is the ability of people to enter external doors without having their access controlled and validated. A covered entity should strongly consider locking entry from the outside for any door that is not manned by security or reception.

Maintenance Records

A covered entity should "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)."[63]

[59] 45 C.F.R. §164.310(a)(1).

[60] 45 C.F.R. §164.310(a)(2)(i).

[61] 45 C.F.R. §164.310(a)(2)(ii).

[62] 45 C.F.R. §164.310(a)(2)(iii).

[63] 45 C.F.R. §164.310(a)(2)(iv).

CCH-EXP, Health-Comp-Manual, **¶20,825 Workstation Use**
Workstation Use

The Workstation Use Standard requires a covered entity to "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 has no implementation specification and therefore must be implemented as written.[64]

[64] 45 C.F.R. §164.310(b).

CCH-EXP, Health-Comp-Manual, **¶20,826 Workstation Security**
Workstation Security

The Workstation Security Standard requires a covered entity to "implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."[65] This standard has no implementation specifications and therefore must be implements as written.

[65] 45 C.F.R. §164.310(c).

CCH-EXP, Health-Comp-Manual, **¶20,827 Device and Media Controls**
Device and Media Controls

The Device and Media Controls Standard has four implementation specifications that provide detail on how a covered entity should "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."[66]

Disposal

A covered entity must "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."[67]

It is critical that covered entities dispose of electronic hardware and media in a way that renders any electronic protected health information inaccessible by another person. Various forms of wiping hard drives should be reviewed and employed. Covered entities may also wish to consider destroying the electronic hardware and software before disposing of the material.

Media Re-use

A covered entity must "implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."[68]

Accountability

A covered entity must "maintain a record of the movements of hardware and electronic media and any person responsible therefore."[69]

Data Backup and Storage

A covered entity must "create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."[70]

[66] 45 C.F.R. §164.310(d)(1).

[67] 45 C.F.R. §164.310(d)(2)(i).

[68] 45 C.F.R. §164.310(d)(2)(ii).

[69] 45 C.F.R. §164.310(d)(2)(iii).

[70] 45 C.F.R. §164.310(d)(2)(iv).

CCH-EXP, Health-Comp-Manual, **¶20,828 Introduction**

Introduction

Although the Security Rule is often perceived as a set of technical and technology regulations because it mandates safeguards to protect electronic protected health information, ironically the technical safeguards section of the Security Rule encompasses the smallest portion of the Security Rule.

CCH-EXP, Health-Comp-Manual, **¶20,829 Access Control**

Access Control

The Access Control Standard has four implementation specifications that set out detail on how a covered entity should "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 [under the Information Access Management Standard]."[71]

Unique User Identification

A covered entity must "assign a unique name and/or number for identifying and tracking user identity."[72] Covered entities should not assign the same user identification or password to multiple people. CMS has reiterated this obligation in an FAQ published May 4, 2005 in stating, "the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains electronic protected health information, so that system access and activity can be identified and tracked by user."[73]

Emergency Access Procedure

A covered entity must "establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."[74]

Automatic Logoff

A covered entity must "implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."[75] This specification does not state how long a period of inactivity should be allowed before a work station or information system is automatically logged-off. Circumstances may vary. Many covered entities are allowing no longer than 15 minutes of inactivity before automatic log-off.

However, health care providers often have much shorter inactivity periods for workstations that are in patient care areas or areas with easy access by visitors or patients. In these areas it is not uncommon to find one, two, or three minute automatic log-off triggers.

Encryption and Decryption

A covered entity must “implement a mechanism to encrypt and decrypt electronic protected health information.”[76] This implementation specification is related to so-called “data at rest” and is in relation to information maintained by the covered entity.

[71] 45 C.F.R. §164.312(a)(1).

[72] 45 C.F.R. §164.312(a)(2)(i).

[73] CMS FAQ Answer ID4737.

[74] 45 C.F.R. §164.312(a)(2)(ii).

[75] 45 C.F.R. §164.312(a)(2)(iii).

[76] 45 C.F.R. §164.312(a)(2)(iv).

CCH-EXP, Health-Comp-Manual, **¶20,830 Audit Controls**
Audit Controls

The Audit Controls Standard requires a covered entity to “implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”[77] This standard has no implementation specifications and therefore must be implemented as written.

A covered entity should consider designing an audit mechanism for each information system it utilizes.

[77] 45 C.F.R. §164.312(b).

CCH-EXP, Health-Comp-Manual, **¶20,831 Integrity**
Integrity

The Integrity Standard has one implementation specification that provides details on how a covered entity should “implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”[78]

Mechanism to Authenticate Electronic Protected Health Information

A covered entity should “implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”[79]

[78] 45 C.F.R. §164.312(c)(1).

[79] 45 C.F.R. §164.312(c)(2).

CCH-EXP, Health-Comp-Manual, **¶20,832 Person or Entity Authentication**
Person or Entity Authentication

The Person or Entity Authentication requires that a covered entity "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."[80] This standard has no implementation specifications and therefore must be implemented as written.

[80] 45 C.F.R. §164.312(c)(2).

CCH-EXP, Health-Comp-Manual, **¶20,833 Transmission Security**
Transmission Security

The Transmission Security Standard has two specifications that provide detail on how a covered entity should "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[81]

Integrity Controls

A covered entity should "implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."[82]

Encryption

A covered entity should "implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."[83] Unlike the encryption specification discussed in ¶20,829 above, here the Security Rule is addressing electronic protected health information that is being transmitted over an electronic communications network, such as via e-mail.

[81] 45 C.F.R. §164.312(e)(1).

[82] 45 C.F.R. §164.312(e)(2)(i).

[83] 45 C.F.R. §164.312(e)(2)(ii).

CCH-EXP, Health-Comp-Manual, **¶20,834 Business Associate Issues**
Business Associate Issues

A covered entity violates the Security Rule if it knows of a pattern of activity or practice of its business associate that constitutes a material breach or violation of the business associate's obligations under the business associate agreement or other arrangement, as the case may be, unless the covered entity takes reasonable steps to cure the breach or end the violation.[84] If such steps are unsuccessful, the covered entity must terminate the contract or arrangement, if feasible. The covered entity must report the problem to the Secretary of HHS if termination of the business associate agreement or arrangement is not feasible.

[84] 45 C.F.R. §164.502(e)(1)(iii).

CCH-EXP, Health-Comp-Manual, **¶20,835 Requirements for Group Health Plans**
Requirements for Group Health Plans

A group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan, except in the following limited situations:[85]

1) to disclose summary health information to the plan sponsor for the purpose of the plan sponsor obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or modifying, amending or terminating the group health plan;

2) to disclose electronic protected health information to the plan sponsor regarding whether an individual is participating in the group health plan has enrolled or has disenrolled; and

3) when authorized by the individual about whom the electronic protected health information pertains.

If the plan documents must be amended, they must be amended to incorporate provisions similar to those required of a business associate agreement as discussed in ¶20,823 above.

[85] 45 C.F.R. §164.314(b).

CCH-EXP, Health-Comp-Manual, **¶20,836 Documentation Requirements**

Documentation Requirements

Covered entities must have written policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule.[86] Covered entities may change their policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Rule.

Covered entities must also maintain a written record of all actions, activities, and assessments that are required to be documented by the Security Rule.[87] The Rule permits the written record to be in electronic form.

Covered entities must retain each piece of required documentation for six years from the date of its creation or the date when it was last in effect, whichever is later.[88] For example, a policy statement that was effective as of April 20, 2005 might be amended effective January 1, 2006. In that case, the written (or electronic) documentation of the April 20, 2005 version of the policy must be retained by the covered entity until December 31, 2011, i.e., six years after it was last in effect.

[86] 45 C.F.R. §164.316(a).

[87] 45 C.F.R. §164.316(b)(1)(i).

[88] 45 C.F.R. §164.316(b)(2)(i).