1-1-2007

The Security Rule

Stephen M. Jerbic
San Jose State University, m.jerbic@riskgenesis.com

Stephen S. Wu

Recommended Citation

Stephen M. Jerbic and Stephen S. Wu. "The Security Rule" *A Guide to HIPAA Security and the Law* (2007): 25-92.

A Guide to HIPAA Security and the Law was a project of the American Bar Association's Section of Science & Technology Law.

5 The Security Rule

by Mike Jerbic and Stephen Wu

A. GENERAL RULES

In general, the Security Rule ensures that Covered Entities protect the confidentiality, integrity, and availability of electronic Protected Health Information.[1] "Confidentiality" means that information is not made available or disclosed to unauthorized persons or processes.[2] In other words, Covered Entities must protect ePHI against interception and other unauthorized access or use by people or processes. The term "integrity" refers to safeguards to prevent the unauthorized alteration or destruction of information.[3] That is, security mechanisms should provide assurances that no information has been tampered with or corrupted, or at least assurances that if tampering or corruption occurs, the alteration can be detected. Detecting tampering or corruption ensures that Covered Entities are not relying on unreliable information. "Availability" refers to information being accessible and usable upon demand by an authorized person.[4] The availability concept provides assurances that information is there when it is needed. An illustration of this concept is the "denial of service" attack in which the at-

1. 45 C.F.R. § 164.306(a)(1).
2. *Id.* § 164.304.
3. Id.
4. Id.

tacker makes a Web site or other system inaccessible by flooding it with bogus transactions or requests for information. Assurances of availability to fight denial of service attacks help to ensure that the Web site or other service is available when users wish to access it.

In addition to these general principles, the Security Rule requires Covered Entities to:

- Protect against reasonably anticipated security threats;
- Protect against reasonably anticipated uses or disclosures that violate the Privacy Rule;
- Ensure that its workforce complies with the Security Rule;[5] and
- Periodically review and modify security measures to maintain continuing compliance.[6]

The Security Rule recognizes that there is no "one size fits all" method of securing information and systems. The rule does not require a single set of security measures for all Covered Entities. To the contrary, the Security Rule permits a great deal of flexibility. In deciding on which specific security measures to implement, Covered Entities have some discretion to select security measures that "reasonably and appropriately" implement the regulations.[7] The regulations permit Covered Entities to make this decision by considering the following factors:

- The size, complexity, and capabilities of the Covered Entity;
- The Covered Entity's technical infrastructure, hardware, and software security capabilities;
- The cost of security measures; and
- The probability and criticality (likelihood of occurrence and magnitude of harm) of potential risks to the electronic Protected Health Information.[8]

The structure of the regulations comprising the Security Rule consists of numerous security standards that are, in essence, a series of high-level requirements that Covered Entities *must* meet.[9] To flesh out the details of the Security Rule and its standards, the regulations present a series of implementation specifications. Two types of implementation

5. *Id.* § 164.306(a)(2)-(a)(4).
6. *Id.* § 164.306(e).
7. *Id.* § 164.306(b)(1).
8. *Id.* § 164.306(b)(2)(i)-(b)(2)(iv).
9. *Id.* § 164.306(c).

specifications appear in the regulations. First, some implementation specifications are required,[10] and a Covered Entity *must* implement required implementation specifications.[11] The exact mechanisms to do this are not specified because, as mentioned above, Covered Entities have the flexibility to choose security measures that "reasonably and appropriately" implement the required implementation specifications.

The second type of implementation specification is called addressable.[12] Addressable implementation specifications *are not requirements*. Instead, Covered Entities must go through a process by which they analyze whether a particular addressable implementation specification is reasonable and appropriate in view of its likely contribution to the security of ePHI.[13] If the addressable implementation specification is reasonable and appropriate under the circumstances, then the Covered Entity must implement it.[14] If it is not reasonable and appropriate, then the Covered Entity need not implement it. Nonetheless, it must instead:

- Document why it would not be reasonable and appropriate to implement it; and
- Implement an equivalent alternative safeguard, if it is reasonable and appropriate.[15]

B. ADMINISTRATIVE SAFEGUARDS—*SECTION 164.308*

> ***Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.***[16]

Administrative safeguards are the nontechnical measures that an organization's management establishes regarding acceptable em-

10. *Id.* § 164.306(d)(1).
11. *Id.* § 164.306(d)(2).
12. *Id.* § 164.306(d)(1).
13. *Id.* § 164.306(d)(1)(i).
14. *Id.* § 164.306(d)(1)(ii)(A).
15. *Id.* § 164.306(d)(1)(ii)(B)(1)-(d)(1)(ii)(B)(2).
16. *Id.* § 164.304 (definition of "administrative safeguards").

ployee conduct, personnel procedures, and correct technology usage within the enterprise. In the parlance of information security professionals, safeguards consist of:

- Policies—Management's documented statement of intent.
- Standards—Policy-mandated technical measures the organization will use to solve specific problems. Standards often specify the appropriate use of technology.[17]
- Guidelines—Suggested, usually strongly suggested, behavior recommendations that usually will be followed.
- Procedures—Documented methods for implementing mandated processes.

These safeguards range from policies, which are the most general, to procedures, which are the most specific. Standards and guidelines are in between. Addressable implementation specifications are akin to guidelines in the sense that both are not mandatory, but they are not identical. The Security Rule has a specific definition for, and procedures for applying, addressable implementation specifications.[18]

The Security Rule requires the Covered Entity to establish (through its management's approved documentation) and implement (carry out and enforce) policies and procedures for administrative safeguards in these areas:[19]

- security management process
- assigned security responsibility
- workforce security
- information access management
- security awareness and training
- security incident procedures
- contingency plans
- evaluation

The subsections of this Section 5.B discuss each of these areas in turn.

---

17. This use of the word "standard" is in the engineering sense of the word and is different from references to regulations or groups of regulations. *See* Section 3.A note 5 *supra*.
18. *See* Section 5.A *supra*.
19. 45 C.F.R. § 164.308(a).

The Security Rule extends to business associate contracts or other arrangements,[20] for example, Covered Entities using outsourced service providers to process ePHI.

1. Security Management Process (Standard)—Section 164.308(a)(1)(i)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

The security management process section and its implementation requirements below are the foundation of all of the administrative security safeguards. Keys to the management process are:

- management support at the highest levels
- initially defining policies and procedures
- execution and enforcement of policies and procedures
- maintenance, periodic update, and diligent refinement of policies and procedures

No single policy will fit all Covered Entities, and the rule specifically recognizes that security policies must align with business imperatives. ePHI security policy management is part of overall Covered Entity health care business management. Many organizations will already possess a current security policy of some form. A HIPAA-compliant security policy, can augment the existing policy and enhance the organization's security infrastructure.

A Security Rule-compliant security policy must contain at least the following four required sections: risk analysis, risk management, sanction policy, and information system activity review. The policy containing the process and results of the risk assessment should be in writing, which may be in electronic form.[21]

(a) Risk Analysis (Required)—Section 164.308(a)(1)(ii)(A)

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

20. *Id.* § 164.308(b)(1).
21. *Id.* § 134.316(b)(1).

At the heart of HIPAA compliance is an assessment of confidentiality, integrity, and availability risks to ePHI. The Security Rule does not state what a compliant risk analysis contains, leaving the content of the risk analysis to the discretion of the Covered Entity. The Covered Entity may benefit from reviewing previous risk analyses, security audits, and other assessments to compare the current risk profile with previous ones.

Information security professionals, however, generally use four components for their risk analyses: asset identification and valuation, threat identification, vulnerability identification, and risk identification.

Asset Identification and Valuation

The term "assets" refers to items of value to the Covered Entity. Assets include (among other things) computer hardware, software, records, and other information. Asset identification and valuation involve inventorying and listing assets to be considered within the scope of the risk assessment. Under the Security Rule, the focus is on listing those assets containing, processing, or transmitting ePHI. In short, the Covered Entity must know what ePHI it possesses and where it is located and communicated.

In order to identify the risks to ePHI accurately and limit the scope of the risk assessment, the assets analyzed should be limited to avoid sweeping in threats and vulnerabilities relevant to the larger organization or application but not to ePHI. Once identified, the Covered Entity needs to assign an appropriate value to each asset, which can be monetary or simply a qualitative measure of the asset's value (e.g., high, medium, or low). The value of the information should account for its sensitivity.

Threat Identification

The Covered Entity should determine the threats facing its ePHI-related assets. A threat is a possible future negative event that can damage an asset vulnerable to such a threat. Information security threats have the potential to compromise the confidentiality, integrity, or availability of information. Threats may be intentional, such as a hacker attempting to break into a network. Additionally, though, threats may be inadvertent, such as the mistyping of an e-mail address, which may be attributable to natural human carelessness or fatigue. Threats may extend beyond human conduct, whether intentional or not, to natural or physical phenomena. For instance, hurricanes, floods, fires, and earthquakes pose

threats to the availability of information when they strike data centers and the equipment operating in them.

In identifying threats, risk assessors may be able to identify a large range of threats. Some will be severe and likely threats. Others will be more remote and unlikely. The threats that are reasonably anticipated are the ones on which risk assessors should focus most of their attention.

Vulnerability Identification

The Covered Entity should next ascertain the extent to which it is vulnerable to certain threats. The Covered Entity should determine what safeguards are currently in place to address specific threats. They should also assess the strengths and weaknesses of their safeguards.

A vulnerability is a weakness in an asset that allows a threat to damage that asset. This weakness can stem from the lack of a safeguard designed to protect the asset, a weakness in the safeguard, or in a characteristic of the asset itself. Threats have the potential of exploiting these weaknesses to damage the confidentiality, integrity, or availability of the asset. Vulnerabilities, however, only exist in the context of specific threats. Thus, the Covered Entity must carefully consider which threats are relevant to them and their ePHI when assessing the vulnerability of an asset to a particular threat.

Risk Identification

The risk identification step analyzes risk based on the likelihood that a threat will exploit a vulnerability and the impact that event would have on the vulnerable asset. The Covered Entity can use existing questionnaires, interviews with experts, past history, and other means to determine the risks the organization may encounter. The Covered Entity should document potential risk elements as part of its risk management process. High risks are those involving threats that occur frequently and/or exploit vulnerabilities of high-value assets. Low risks are those where a minor vulnerability may expose a low-value asset to unlikely or infrequent compromise or loss. Even when the risk identification step is completed, there is a remaining "unidentified risk." That is, risks may arise from threats that assessors cannot reasonably discover or identify.

In the process of identifying risks, it may become apparent to risk assessors that the Covered Entity should implement or strengthen certain safeguards. These recommendations can inform the risk manage-

ment process described below.[22] Risk assessors may also be able to identify areas where risk is likely to remain, even after reasonable and appropriate safeguards are put into place.

Security professionals use two analytic methodologies to measure risk: qualitative and quantitative risk analysis.

Qualitative Risk Analysis

Not only does risk analysis involve the evaluation of the probability and frequency that an identified threat will exploit a vulnerability, but it also involves measuring the anticipated impact that exploiting the vulnerability will have on the organization. Each risk is analyzed in terms of its anticipated impact (severity) and its probability or frequency (occurrence). Qualitative risk analysis classifies risks into categories of severity and occurrence such as "low," "medium," and "high." The outcome of this risk analysis may be represented in the table in Exhibit 5-1.

Exhibit 5-1
Qualitative Risk Analysis

Risk	Severity	Occurrence
1	Low	Low
2	Low	Medium
3	Low	High
4	Medium	Low
5	Medium	Medium
6	Medium	High
7	High	Low
8	High	Medium
9	High	High

The exhibit is one example of how assessors can categorize different types of risk. It is merely an example. Note also that the numbers 1-9 are categories and do not necessarily connote a ranking of risk. At

22. *See* Section 5.B.1.b *infra*.

times, for instance, addressing a very high-frequency, low-severity threat (e.g., spam not containing malicious code) may take precedence over addressing a high-severity, rare threat (e.g., a meteor destroying a facility).

The risk-managed organization will categorize possible risks and then focus its energy first on the high-severity, high-occurrence risks. Once the most significant risks are addressed, it can move onto lower risks.

This approach, while conceptually straightforward, is very subjective. In the absence of objective information, senior management often relies heavily upon its judgment to classify risk, making its decisions potentially difficult to justify to auditors, regulators, and other managers. The Covered Entity should carefully document all the objective information, subjective judgment, and other rationales underlying a qualitative risk analysis.

Quantitative Risk Analysis

Some risks lend themselves to an analysis that estimates loss in financial terms. This kind of analysis assesses:

F — the expected or estimated Frequency (events per year) of occurrence of the threat
L — the anticipated Loss from the vulnerable asset of each successful occurrence
V — the probability that the threat successfully exploits a Vulnerability
E — the Expected Loss each year from the identified risk
E = F * L * V

An organization should prioritize risks according to its expected losses. It can address the high risk threats first and move on to lower risk threats later.

Some security professionals, however, point out limitations inherent in a quantitative risk analysis. Obtaining reliable data on the frequency and probability that a threat will exploit a vulnerability can be difficult. Because threats and vulnerabilities vary by organization, widely aggregated risk data may not be useful. Moreover, information security threats, while essentially independent variables, can be influenced by the value of an asset or its vulnerabilities to attack. Conse-

quently, even reliable threat data may not yield accurate estimates of expected losses. Accordingly, in situations where quantitative risk analysis is not possible or meaningful, a Covered Entity may be limited to analyzing its risk in a qualitative fashion.

As mentioned earlier, the Security Rule does not define how an organization must conduct its risk analysis. No matter what approach the Covered Entity takes in analyzing its ePHI security risk, whether qualitative or quantitative, it should carefully document all elements of the analysis and understand that auditors, regulators, and business managers may challenge the results.

Risk assessment is complete once the above steps for asset identification and valuation, threat identification, vulnerability identification, and risk identification have been completed.

(b) Risk Management (Required)—Section 164.308(a)(1)(ii)(B)

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Risk management describes the continuous, iterative process of:

(a) Reviewing the results of the Covered Entity's risk analysis to assess the effectiveness of current safeguards to provide assurances of confidentiality, integrity, and availability of ePHI in light of reasonably anticipated threats, and to identify any gaps in effectiveness that create risk.

(b) Analyzing recent changes to the Covered Entity's environment, including such factors as: (i) implementation of new technology and associated vulnerabilities; (ii) developments in new threat technology; (iii) changes to organizational structure and business goals; and (iv) changes in regulations.

(c) Measuring and prioritizing risks and corresponding mitigation safeguards and other measures, and incorporating them into a Risk Management Plan; and

(d) Implementing those mitigation measures defined in the Risk Management Plan. As mentioned above, the Security Rule permits flexibility in implementing security measures that are "reasonable and appropriate." Accordingly, the Covered Entity must apply its business judgment in managing existing and new risks.

The risk management plan should address how each identified risk is to be managed to an acceptable level. Risks may be prioritized on the basis of degree of risk, magnitude of harm that a threat could cause, the cost to mitigate a vulnerability, business and operational goals and critical needs, and expected effectiveness of mitigation measures. This requirement's objective is to eliminate as much expected loss as is "reasonable and appropriate." The Covered Entity can address any residual expected loss in its security policy. The risk management plan identifies the specific mitigation measures that are taken to address the risks to the confidentiality, integrity, and availability of the Covered Entity's ePHI.

In determining what safeguards are necessary to reduce risks and vulnerabilities to a "reasonable and appropriate" level, the Covered Entity should consider the following factors:

- The size, complexity, and capabilities of the Covered Entity;
- The Covered Entity's technical infrastructure, hardware, and software security capabilities;
- The cost of security measures; and
- The probability and criticality of potential risks to electronic protected health information.[23]

The risk management process results will drive the Covered Entity's further efforts to manage ePHI security. The Covered Entity is not expected to eliminate all risks. Instead, the Security Rule requires the Covered Entity only to manage the risks to an acceptable level, based upon its risk analysis.

When risk management requires the procurement of new hardware, software, or services to implement or strengthen safeguards, the Covered Entity should determine whether the costs are worth the benefits of those new products or services. In addition, the Covered Entity will have to integrate any new purchases with its existing technology, systems, and personnel. Security solutions that address a vulnerability, but disrupt other systems and services, may create more problems than they solve.

Moreover, new technology procurements are not a panacea for complying with the Security Rule. Some security threats may require

23. 45 C.F.R. § 164.306(b)(2).

changes to policy or procedure or more extensive training programs for the Covered Entity's personnel. To comply with the Security Rule, the Covered Entity must consider all sources of risk, including those sources stemming from its people and processes and not just from its technology. In short, there is no "security in a box" that a Covered Entity can simply purchase to have instant compliance with the Security Rule.

(c) Sanction Policy (Required)—Section 164.308(a)(1)(ii)(C)

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

The Covered Entity must have the policies and accompanying procedures in place to take action against individuals who violate its documented security policy. The rule does not state what those sanctions must be, but instead requires them to be reasonable and appropriate. For instance, a Covered Entity may impose discipline for security violations up to and including termination. The purpose of the sanction policy is to hold employees and contractors accountable for their actions.

Implementing a sanction policy involves several steps. First, the policy should be a written policy addressing the different types of sanctions imposed for different types of security violations. The policy should also address procedures for investigating, reporting, and resolving security violations. The Covered Entity should plan in advance what sanctions are appropriate for what kinds of conduct. Second, the Covered Entity must inform its staff of the sanction policy to set expectations of appropriate conduct, deter violations of security policies, and provide fair, advance warning of sanctions that security violations may trigger. Third, Covered Entities should actually implement the sanction policy as violations occur, and implement the policy in a consistent, even-handed manner.

(d) Information System Activity Review (Required)—Section 164.308(a)(1)(ii)(D)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

This requirement specifies that the Covered Entity must set up its information system monitoring or audit function and also must review the data collected. The procedures in the Covered Entity's security policy must define what information is collected and when it is to be reviewed. The sanction policy should describe what the implications are for discovered abuse/misuse. The purpose of this requirement is to detect security incidents and breaches and provide the evidence needed to take remedial actions.

Covered Entities should consider the following factors when establishing policies concerning the review of information system activity. First, they should designate a person or group to take charge of the review process for various items of activity information. Second, they should determine how often personnel can review activity information and how much of the information personnel can review practically. If the activity information, such as log files, is too voluminous to review in total, Covered Entities may be able to use automated tools to alert responsible staff members of especially serious events. Finally, Covered Entities should address the need to retain in a secure fashion activity information that may become evidence in later legal proceedings to provide assurances against falsification, tampering, and corruption.

2. Assigned Security Responsibility (Standard)—Section 164.308(a)(2)

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

One of the required administrative safeguards is the Covered Entity's documented appointment of a chief security official or other responsible official who has direct, accountable responsibility for Security Rule-required policies and procedures. Note that this official is not required to have policy approval responsibilities, but rather just policy development and implementation responsibilities. This person need not be the same individual responsible for the Privacy Rule.

The Covered Entity's documentation should include a description of the security official's responsibilities and tasks. The Covered Entity should, in turn, notify its staff and business associates of the security official's role. Finally, the Covered Entity should tell staff and business associates of the security official's contact information

to ensure proper and timely reporting of security incidents to the security official. Staff and business associates should know what and how they should communicate with the security official.

3. Workforce Security (Standard)—Section 164.308(a)(3)(i)

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

People are both the weakest link and greatest threat in any security program. To address this combined vulnerability and threat, the Covered Entity must institute policies, procedures, and standards for ensuring that the security risk of the workforce itself is managed. Those workers without the need to access ePHI should not be given access rights, and workers without explicit access rights must be denied access to ePHI. To comply with these administrative safeguards, the entity, through administrative procedures, should meet the following three specifications: authorization and/or supervision, workforce clearance procedure, and termination procedures.

(a) Authorization and/or Supervision (Addressable)—Section 164.308(a)(3)(ii)(A)

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

This specification calls for the implementation of workforce security procedures that define and address allowable access, where such procedures are reasonable and appropriate. Under the standard of the previous subsection, management must document the procedure for granting access to ePHI. This specification addresses how a Covered Entity grants access rights to ePHI. Further, Covered Entities should properly supervise those who do have access.

For instance, the Covered Entity should have a clear reporting structure to establish who has authority to make what decisions about staff access to ePHI under what circumstances, and who has the re-

sponsibility to supervise staff members. The Covered Entity should train staff members concerning that reporting structure and the authorization process. A helpful step to having a clear reporting structure is having written job descriptions for each position that identify and define levels of access to ePHI to be granted to that position. Descriptions of levels of access should address the appropriateness of granting rights such as reviewing records, creating new records, modifying records, and deleting records; the circumstances for exercising these rights; the purposes for proper exercise of these rights; and the types of records to which these rights should apply.

(b) Workforce Clearance Procedure (Addressable)—Section 164.308(a)(3)(ii)(B)

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Under the workforce security standard, management must define and document the criteria and procedure for granting ePHI access to those employees who need it as part of their job responsibilities. Under this addressable implementation specification, a Covered Entity must (if reasonable and appropriate) implement procedures to ensure that it hires trustworthy and competent staff members for a position whose job description entails access to ePHI. A Covered Entity can more efficiently make a determination of the appropriateness of access to ePHI before hiring a staff member, in contrast to hiring the person and making a later determination about the appropriateness of access, which may involve the need to terminate an unqualified new hire. Making this threshold determination involves comparing the potential hire's skills, qualifications, background, and experience against the job description to determine whether the potential hire is competent. Checking qualifications can (if reasonable and appropriate) involve checking references and objective sources of information, such as transcripts from educational institutions, to make sure that the potential hire does, in fact, possess the qualifications he or she purports to have.

Determining appropriate hires also might include background screenings and other assessments to determine whether a particular individual should have access to ePHI. For instance, a criminal back-

ground check may be reasonable and appropriate for certain positions. Such checks could reveal that a candidate for a position with access to ePHI has convictions for fraud, suggesting that the candidate is not trustworthy. The Covered Entity can use that information in deciding which candidate to choose for a position.

(c) Termination Procedures (Addressable)—Section 164.308(a)(3)(ii)(C)

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 paragraph (a)(3)(ii)(B) of this section.

This specification aims to prevent the situation of an employee who is terminated or otherwise leaves a Covered Entity but is still able to access ePHI. This situation may occur because the information technology (IT) security staff is not advised of the termination, or if aware, neglects to disable the departing employee's information system access. A failure to terminate departing employees' access leaves the Covered Entity's systems vulnerable to the departing employee's misuse and abuse at a particularly risky time—right after an employee is terminated. This addressable specification calls for the Covered Entity to have procedures to manage this risk if reasonable and appropriate. One example is a set of procedures to notify security staff so that access to ePHI can be revoked in a timely manner.

The Covered Entity should have a standard set of procedures for returning property of the Covered Entity, including keys, identification badges, cards used for physical access to a facility, and tokens for access to IT resources. In addition, the Covered Entity should have procedures in place to transition ePHI under the sole control of the departing employee to staff members who are staying, so that the Covered Entity does not lose access to any ePHI. Finally, the Covered Entity's procedures should include provisions to terminate user accounts for accessing IT systems containing ePHI. Procedures may need to vary based on the circumstances of the termination. That is, the risk of misuse following a voluntary departure or retirement is lower than in situations where an employee is laid off or fired for cause. Whatever standard procedures the Covered Entity establishes, the Covered Entity should apply them consistently and even-handedly when terminating employees.

In some instances, the Covered Entity may use independent contractors to perform certain functions. This specification speaks of "employment of a workforce member," which seems to imply an employer-employee relationship between the Covered Entity and the workforce member. Nonetheless, Covered Entities should apply the practices described in this subsection to departing independent contractors who have access to PHI.

4. Information Access Management (Standard)—Section 164.308(a)(4)(i)

> ***Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.***[24]

This section directs a Covered Entity's management to develop, document, and implement policies and procedures to limit access to ePHI. Implementation specifications cover three specific areas, one required, and two of them addressable, as discussed in the subsections below.

(a) Isolating Health Care Clearinghouse Functions (Required)—Section 164.308(a)(4)(ii)(A)

> ***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 larger organization.***

A Covered Entity must determine whether it performs any health care clearinghouse functions. If so, it must erect an ePHI information flow barrier or "Chinese wall" between the health care clearinghouse function and any of the other business functions of the parent organization. The Covered Entity should scrutinize areas where overlap or crossover of ePHI may occur, such as information systems and resources, physical facilities, and staff members. If reasonable and appropriate, the Covered Entity may want to isolate the network and information systems resources of the clearinghouse function entirely from systems serving other operations. The Covered Entity should also include, as a component of its security awareness training, proper

24. 45 C.F.R. §§ 164.500-164.534 (Privacy Rule).

procedures for isolating the ePHI of the clearinghouse from the rest of the organization.

(b) Access Authorization (Addressable)—Section 164.308(a)(4)(ii)(B)

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.

The administrative policies and procedures described in this implementation specification govern how Covered Entities grant and control access privileges for applications, workstations, and ePHI to authorized people in the organization. They must be implemented if they are reasonable and appropriate. When determining who in the organization should access systems, programs, databases, or other intermediaries to ePHI, management should consider policies that limit access to the minimum number of people and minimum extent necessary for employees to perform their job. Granting privileges that exceed the minimum required for proper job performance can add risk to ePHI security and privacy.

Under some circumstances, a contractor, business associate, patient, or other outside party may have a need to know ePHI concerning the patient. The Covered Entity should make an assessment as to whether that access is appropriate. Even if granting access to a user is appropriate, the Covered Entity should limit that access to the minimum level necessary for the outsider to perform needed or desired functions.[25]

Part of the determination of whether access is appropriate involves "authenticating" the proposed user: ensuring that the person seeking access is who he or she claims to be. An authentication process can have two separate components, depending on the need for rigor in the authentication process. First, an authentication process includes ensuring that the person to be granted access corresponds to a real-world identity. For instance, if a Covered Entity wishes to hire a new physician purporting to be Jane Smith, authentication procedures can determine whether there is, in fact, a real Jane Smith who is a physician.

25. The procedures for determining levels of access appropriate for certain roles is described in Section 5.B.3 *supra*.

This type of authentication prevents people from using a fictitious identity.

Second, assuming that a real-world identity exists, the authentication process can ensure that the person using a system or gaining access to ePHI does, in fact, correspond to the real-world identity. For instance, in the example of physician Jane Smith, authentication procedures can confirm that the person seeking the position is, in fact, Jane Smith the physician. The purpose of this kind of authentication is to prevent the impersonation of a real person.

In addition, even if the Covered Entity hires and sets up an account for the real Jane Smith, the Covered Entity should have procedures to ensure that a person seeking access to ePHI on its information systems at a given time is, in fact, the same Jane Smith. In other words, the Covered Entity should implement a mechanism to control access. Technical safeguards should be in place to control access. Technical safeguards can control access to a given workstation, program, process, or other system. Covered Entities can also use technical safeguards to ensure that only authorized users complete certain kinds of transactions.

Various technical measures are available to control access. They include user name-password combinations, access tokens such as smart cards, and biometric devices such as fingerprint readers. Technical access control safeguards are discussed in more detail below in Section 5.D.1.[26]

(c) Access Establishment and Modification (Addressable)—Section 164.308(a)(4)(ii)(C)

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.

People who move from job to job within an organization tend to accumulate information access privileges along the way. This addressable provision calls for policies and procedures for the documented establishment and periodic review of an employee's ePHI access privileges to ensure that the individual has appropriate access privileges to per-

26. *See* 45 C.F.R. § 164.312(a).

form current functions. These policies and procedures must be implemented if they are reasonable and appropriate. Granted privileges should be the minimum needed for an individual to perform his or her job.

From time to time, the Covered Entity should review the individual's access privileges. When discovered, unnecessary privileges should be removed. By contrast, promotions or increases in responsibilities may require increasing an individual's access privileges. Records concerning which staff members have what access privileges should be protected against unauthorized alteration, corruption, or tampering.

5. Security Awareness and Training (Standard)—Section 164.308(a)(5)(i)

Implement a security awareness and training program for all members of its workforce (including management).

A Covered Entity must have a comprehensive security awareness and training program. Security training should be mandatory for all new hires having access to ePHI. People cannot perform their duties securely unless they are familiar with the entity's security policies and procedures. Awareness allows employees to grasp the importance of security and its role in protecting privacy. Training focuses on how to use the security features and maintain a secure information processing environment.

Even after a new hire has received training, the new hire should know how to access instructional material on security procedures for later reference and people to whom the new hire can direct security questions or report incidents. Moreover, the Covered Entity should apply and enforce policies and procedures covered in the security awareness and training consistently and in an even-handed fashion.

Implementation of this requirement consists of four specifications as described below.

(a) Security Reminders (Addressable)—Section 164.308(a)(5)(ii)(A)

Periodic security updates.

Training and awareness are continuous, not one-time events. The Covered Entity must, where reasonable and appropriate, have an ongoing program of periodic security awareness and training. Its goal should be

to keep staff up-to-date on the latest risks and threats the system is facing, as well any changes in the Covered Entity's security programs, policies, or procedures.

The Covered Entity should schedule periodic refresher courses on security awareness. In addition, the Covered Entity may, from time to time, uncover an unusually urgent emerging threat. In that case, it may be reasonable and appropriate to hold immediate training in methods to address vulnerabilities exploitable by the threat.

The Covered Entity can also make use of refresher training sessions to make adjustments in the type and scope of training provided. The Covered Entity should assess the effectiveness of its training. If deficiencies appear in its training program, it should supplement its instruction at the next appropriate opportunity for refresher training.

(b) Protection from Malicious Software (Addressable)—Section 164.308(a)(5)(ii)(B)

Procedures for guarding against, detecting, and reporting malicious software.

If reasonable and appropriate, the organization must have a policy and procedure on how it will protect itself from malicious software. Malicious software can be anything that affects ePHI confidentiality, integrity, and availability. Examples of malicious software include viruses, worms, and Trojan Horses. Software can enter the environment from many sources including e-mail, employee-installed software, and Web sites.

The Covered Entity's security awareness and training should include instruction on avoiding harm from malicious software. Many of the sources of malicious software rely on "social engineering," that is, nontechnical means of bypassing security safeguards by prompting some response by a legitimate user. For instance, some virus-laden e-mails recite that their attachments contain images of a popular celebrity. These messages trick users, who want to see the images, into clicking on the attachment. Clicking on the attachment then executes code that installs the malicious software. Some training may also be important to prompt users to seek out patches and updates to anti-virus software, or at least not defeat or obstruct automated processes to install patches and updates.

(c) Log-in Monitoring (Addressable)— Section 164.308(a)(5)(ii)(C).

Procedures for monitoring log-in attempts and reporting discrepancies.

The Covered Entity must, where reasonable and appropriate, have appropriate procedures for monitoring attempts to log into systems or applications that contain or can access PHI and for reporting anomalous events. Examples of these events include:

- Unusual times for a workstation to be active or logged in (such as well after business hours or during an employee's off time), which may indicate an employee may be trying to get protected information outside of the scrutiny of his/her supervisor, or an attacker may be attempting to gain access.
- Unusually high numbers of failed log-in attempts (which might indicate that an attacker is trying to log in, does not know the password, but is attempting to guess the password).

Training is helpful in the area of log-on monitoring to inform users how to report log-on anomalies. One example of an anomaly is a user arriving at work and seeing that someone has already gained access to the user's account on the user's workstation. Personnel should also report anomalies pursuant to the Covered Entity's security incident procedures.[27]

(d) Password Management (Addressable)— Section 164.308(a)(5)(ii)(D)

Procedures for creating, changing, and safeguarding passwords.

Covered Entities must, where reasonable and appropriate, implement password security procedures. These procedures will likely require all personnel to bear the responsibility for maintaining secure passwords. Passwords may have security standards themselves, such as:

- Minimum length
- Complexity (e.g., required numeric and nonalphabetical characters, lower and upper case letters, etc.)

27. *See* Section 5.B.6 *infra*.

- Difficulty of guessing (e.g., avoidance of dictionary words, maiden names, pets' names, spouse's name, etc.)
- Minimum and maximum usage time dictating when they must be changed
- Precluding a user from reusing passwords that the user had previously used

Password management and password confidentiality policies and procedures directly affect the security of the accessed system or application. If the Covered Entity makes use of passwords for access control, it should include instruction in the choice and updating of passwords that are hard to compromise. If reasonable and appropriate, the Covered Entity may wish to make use of automated tools to enforce secure password use. For instance, some tools require users to change passwords after a defined time has elapsed.

6. Security Incident Procedures and Responses—Section 164.308(a)(6)

(a) Security Incident Procedures (Standard)—Section 164.308(a)(6)(i)

Implement policies and procedures to address security incidents.

The first step in implementing policies and procedures for security incident handling is developing and establishing policies and procedures. Moreover, the personnel developing the policies and procedures should understand what a "security incident" is. The Security Rule defines "security incident" as follows: "Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[28]

The Covered Entity should establish a person or team of people to develop incident-handling policies and procedures. Team members should have sufficient experience and training in incident response to create sound documentation. Further, the policies and procedures resulting from the team's work should have the support and priority from management to ensure their smooth implementation.

28. 45 C.F.R. § 164.304.

In addition to the team of people to *develop* the incident-handling policies and procedures, the policies and procedures should identify the team of people to *implement* the procedures and *respond* to incidents. For instance, Covered Entities should consider the roles of management, operational personnel, information technology personnel, public relations, and in-house or outside attorneys when establishing policies and procedures.

The Covered Entity should identify the types of incidents that may occur, and plan and document how it should react to each type of incident. The Covered Entity's risk assessment involves identifying threats to ePHI. Thus, assessors can help develop incident-handling policies by informing the drafters of the types of security incidents likely to result from these threats.

Some security incidents that require organizational monitoring and response were already specified in the Log-in Monitoring section above.[29] The organization must go further than log-in monitoring, however, and provide a procedure to address any security incident it discovers. Procedures should address proper reporting of the incident, communications of proper response, implementing the proper response, evidence preservation, and post-incident assessment and remediation to detect, deter, and mitigate future similar incidents. Communications may include discussions by management and public relations personnel with affected parties outside the organization and the media to allay concerns and provide information concerning the Covered Entity's planned response. In addition, Covered Entities should determine whether a security incident triggers reporting requirements under a non-HIPAA law. One such law is California's breach notification law, SB 1386.[30] Other jurisdictions have similar notification laws.

Once personnel develop the policies and procedures, the Covered Entity should implement them. It should make personnel aware of its provisions and clearly communicate the incident-reporting procedures. As incidents arise, personnel should consistently apply the policies and procedures.

After the Covered Entity implements the policies and procedures and accrues experience in their workability, it should periodically review and update them to ensure they are effective and practical. The

29. *See* Section 5.B.5.c *supra*. *See* 45 C.F.R. § 164.308(a)(5)(ii)(C).
30. Cal. Civil Code § 1798.82, 1798.84.

policy development team should seek guidance from operational personnel, who may have advice on improving the effectiveness and efficiency of the incident-handling procedures. The Covered Entity should maintain documentation concerning how well the policies and procedures worked, any needed improvements, and steps taken to improve policies and procedures.

(b) Response and Reporting (Required)— Section 164.308(a)(6)(ii)

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.

This part of the rule requires that a security incident response program be in place. Security awareness and training make discovery of these kinds of events every employee's responsibility. Covered entities must determine when a security incident has occurred, or at least when it suspects an incident has occurred. Moreover, personnel should be trained to follow through with reporting procedures pursuant to the incident-handling policies and procedures.

As a response to incidents, Covered Entities will have to take steps first to find out exactly what happened. Only when the incident response team has the facts can it make an informed decision on a response. The Covered Entity must also take practicable steps to mitigate the effect of incidents. Mitigation may take the form of closing a vulnerability that caused the incident, retrieving information that was lost or misappropriated, implementing a new security safeguard, or strengthening an existing safeguard.

A response should also include reporting of the incident. Personnel should report the incident to management internally. Also, external reporting may be appropriate to allay the concerns of affected parties outside the organization. In addition, external reporting may be required by non-HIPAA law such as California's SB 1386, as mentioned above.

In any event, Covered Entities must document incident reporting and handling. Documentation can enable the Covered Entity to make a record of what happened, assist in managing future efforts to respond to the incident, and facilitate remedial actions to prevent similar incidents in the future. Covered Entities should also preserve any evi-

dence of the incident that may assist in legal proceedings arising from the incident.

7. Contingency Plan (Standard)—Section 164.308(a)(7)(i)

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Information security personnel refer to requirements of this type as business continuity planning and/or disaster recovery. The disaster stemming from Hurricane Katrina in the southeastern United States underscores the importance of having recovery procedures in place. Business continuity/disaster recovery consists of:

- Business impact assessment and analysis to identify critical business processes, services, and operations that need disaster recovery protection and to establish priorities and objectives for business continuity.
- Business continuity plan development to determine how critical business processes will maintain operations during an emergency or after a disaster.
- Maximum allowable downtime of critical business processes, which determines the requirements for contingency planning, subsequent implementation, and disaster recovery; for example, a hospital needs to maintain patient care at all times, but may be able to tolerate some delay in processing administrative tasks.

The contingency plan must ensure that ePHI confidentiality, integrity, and availability can survive any reasonably predictable emergency event. The Covered Entity's risk assessment should identify emergencies that threaten the availability of ePHI. Measures to respond to a disaster must be cost-effective and practical.

As with security incident policies and procedures, a Covered Entity should identify a person or assemble a team to develop business continuity/disaster recovery policies and procedures. The personnel responsible for developing and/or implementing the policies and procedures should have the experience and management support necessary to execute their responsibilities. Management, operational

personnel, information technology personnel, public relations, and in-house or outside attorneys may all have appropriate roles in implementing business continuity/disaster recovery policies and procedures.

In addition, when a disaster occurs, the Covered Entity should put these policies and procedures into action. It should make personnel aware of them in security training. Also, the Covered Entity should have procedures for periodically assessing and reviewing their effectiveness in order to incorporate improvements and updates.

(a) Data Backup Plan (Required)—Section 164.308(a)(7)(ii)(A)

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

The loss of ePHI can disrupt the operation of a Covered Entity. Having a backup copy of ePHI available may prevent such disruption. Under this implementation specification, the Covered Entity must develop policies and procedures governing the backup and retrieval of ePHI. Data backup planning and execution involves more than occasionally making a copy of ePHI and storing it somewhere. Backup planning and implementation should be a formal process that includes the planning of:

- Backup frequency and maximum allowable data loss. The backup frequency (e.g., once per week, once per day, once per hour) and the location of the backup media determine the maximum allowable data loss (the amount of data that wasn't backed up, but now due to the emergency or other incident is not retrievable).
- Maximum time to restore. This metric determines how long it will take to move the backup copy into service. Different methods of storage—tape, optical disk, etc.—require different amounts of time to restore.

Policies and procedures should identify people who are responsible for performing the backup and retrieval functions. Moreover, security training should include procedures for users to take to make appropriate backups and to prevent the loss, destruction, or corruption of ePHI.

ePHI backups need the same security protection as ePHI in its primary (production) systems for normal use. Backup policies and

procedures must establish safeguards for backup data that are of equivalent strength to safeguards protecting production services.

All backup copies must be maintained and be recoverable. Maintenance and recoverability include the following:

- Proper backup media storage to ensure recoverability. All storage media have their specific physical (temperature, humidity, etc.) requirements to ensure recoverability years, even decades after initial backup. All backup media must be physically stored in a manner consistent with these requirements.
- Maintenance of restoration technology itself. With the rapid change of storage and retrieval technology, Covered Entities have to plan how they will maintain recoverability of their backups as storage technology continues to evolve.

(b) Disaster Recovery Plan (Required)—Section 164.308(a)(7)(ii)(B)

Establish (and implement as needed) procedures to restore any loss of data.

The purpose of maintaining backups of ePHI is to have the backup copies available if the data on primary systems are unavailable. The Covered Entity can use the backup copy to restore the data to the primary systems or systems established for emergency mode operation. Restoration of the data permits the Covered Entity to continue operations.

This specification requires the Covered Entity to document procedures governing how it restores lost data. The Covered Entity must then implement such procedures. The Covered Entity's recovery/continuity plan should include how data will be restored on both its primary (production) site and its contingency (emergency) site. Data recovery policies and procedures should work together smoothly with backup policies and procedures.

(c) Emergency Mode Operation Plan (Required)—Section 164.308(a)(7)(ii)(C)

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.

The ability to maintain operations during an emergency or on-going disaster requires substantial planning and preparation. The Covered Entity must incorporate these plans into appropriate polices and procedures. Contingency planning should identify and prioritize which operations need to be continued during emergency mode operation, and which operations are not necessary to continue during emergency mode.

In planning emergency mode operation, the Covered Entity should consider, among others, the following variables:

- Selecting an appropriate site to process and store ePHI during emergency mode operation and configuration of systems at the chosen site.
- Time to load and start service at the site used as a backup (contingency site) to the primary site.
- Security of operations at the contingency site before, during, and after the disaster.
- Operations at the contingency site.
- Transition back to the primary site after the disaster is over, including an ePHI backup for restoration at the primary site.
- Disaster Plan maintenance—periodic review and any necessary updating.

Large Covered Entities may find it reasonable and appropriate to have a "hot site" recovery location where backup information systems can provide services to ensure continuity. A hot site is a dedicated facility, remote from the Covered Entity's primary facility, which can handle operations in the event a disaster makes the primary facility unavailable. Smaller Covered Entities may not find it reasonable and appropriate to incur the expense of equipment sitting idle in a dedicated facility waiting for a disaster, but should have plans for emergency mode operations on-site, if the Covered Entity's primary facility is still usable. For instance, if electric surges damage computer equipment, but the facility is intact, emergency mode may simply involve obtaining temporary or new equipment and operating in emergency mode until systems are restored.

Continued operations in the Covered Entity's primary facility may not be possible, though. For instance, following a flood or earthquake, it may be appropriate for personnel to move salvaged equipment to temporary or new office space and obtain new or leased

equipment to replace damaged systems. Once the primary facility is restored, it may be possible for the Covered Entity to transition back to the primary site.

In any case, regardless of whether the Covered Entity uses a designated hot site, or simply plans for off-site operations in cases where the primary facility is unavailable, the Covered Entity should provide security for ePHI stored and used at the temporary facility. All of the administrative, technical, and physical safeguards that should be in place at the Covered Entity's primary facility should also be in place at the temporary facility. Policies and procedures should document how systems at the temporary facility provide equivalent levels of security.

(d) Testing and Revision Procedures (Addressable)—Section 164.308(a)(7)(ii)(D)

Implement procedures for periodic testing and revision of contingency plans.

To prove the viability of contingency planning, the Covered Entity must (if reasonable and appropriate) periodically test its current plan to verify it will actually work during an emergency. The details of defining and documenting the proper scope, test frequency, and revisions to the contingency plan are left to the discretion of the Covered Entity.

Two types of testing are possible for contingency plans. First, the Covered Entity may conduct a "walk-through" exercise, in which staff meet in a meeting room and discuss how personnel would respond to a disaster. Second, the Covered Entity can actually simulate a disaster by shutting down systems and/or setting up operations in the temporary site for emergency operations. The second type of test will more accurately reflect how the Covered Entity will need to respond to a disaster, but it may not be feasible to conduct that kind of test, or even if feasible, it may not be reasonable or appropriate to conduct that kind of testing in light of the nature of the Covered Entity and the expense involved. In any case, the testing process can be part of the training or refresher training program of the Covered Entity to ensure that personnel are prepared to handle emergencies.

Following the testing process, a Covered Entity will likely gain experience from attempting to replicate the disaster recovery process.

That experience should provide useful feedback for updating and improving policies and procedures established for contingency planning. The Covered Entity should solicit feedback from personnel involved in the testing, and incorporate the feedback into the next version of the documentation.

(e) Applications and Data Criticality Analysis (Addressable)—Section 164.308(a)(7)(ii)(E)

Assess the relative criticality of specific applications and data in support of other contingency plan components.

As discussed above under "Contingency Plan,"[31] the Covered Entity must, if reasonable and appropriate, identify critical business processes, services, and operations involving ePHI, and prioritize them as part of the analysis of its business continuity needs. Some processes, services, and operations are more sensitive to downtime than others. Therefore, the analysis should include a determination of maximum allowable downtime that the Covered Entity can permit and still meet its operational requirements and goals.

Keep in mind that information maintained in a noncritical application may be essential to a critical application. A complete business impact assessment should identify these data dependencies so that the required data can be backed up or otherwise made available to support all critical applications.

8. Evaluation (Standard)—Section 164.308(a)(8)

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this 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 this subpart.

No policy or procedure lasts forever. Management must ensure that policies and procedures are kept current with prevailing security threats, information system vulnerabilities, and security and privacy risks.

31. *See* Section 5.B.7 *supra.*

Management must identify the policy and procedure evaluation frequency (such as once per year, etc.) and document it in the Covered Entity's security policies and procedures. Covered Entities need to maintain version control of all policies and procedures. That is, they must have records of which versions of policies and procedures were written when, and when the policies and procedures were in effect. All employees and regulators should be working with the most recent version of a policy or procedure.

In addition to evaluating periodically the text of the policies and procedures itself, the Covered Entity must also evaluate the implementation of the policies and procedures. That is, the Covered Entity must determine whether and to what extent the real-life procedures and operations of the Covered Entity implementing the documentation do, in fact, comply with the Security Rule. The Covered Entity can evaluate the effectiveness of its policies and procedures by a security assessment.

The Covered Entity can use the Security Rule itself as a source for the initial criteria for a security assessment. Provisions of the Security Rule should act as a checklist to ensure compliance. Environmental and operational changes will then inform what criteria to use in future assessments. For instance, emerging threats and vulnerabilities may make it important to bolster certain assessment criteria.

The standard does not specify who must conduct the security assessment. Larger Covered Entities may find it reasonable and appropriate to hire outside auditors to conduct the assessment, while the expense of outside auditors may not be reasonable for smaller Covered Entities. Smaller Covered Entities may find it more appropriate to use internal personnel to conduct a self-assessment.

In addition to the assessors, it may be useful to include in the assessment process representatives from other groups. For instance, management should oversee the process generally. Management should also communicate its support for the process to ensure that operational personnel understand the Covered Entity's commitment to a thorough assessment. Also, the Covered Entity should consider consulting legal counsel to provide advice concerning the assessment and compare the results of the assessment to the Security Rule to make a bottom-line legal judgment as to whether the Covered Entity complies with the Security Rule or not. Whether or not a Covered Entity complies with the Security Rule is a legal question, which

presumably a lawyer should answer, even if the facts and circumstances of what the Covered Entity is doing to comply can be described by internal or external security personnel. Security consultants helping Covered Entities comply with the Security Rule must avoid engaging in the unauthorized practice of law.

Once the Covered Entity has planned out how the assessment will occur, it must then conduct the assessment. Assessment involves inspecting physical facilities, reviewing outputs from information systems and testing processes to determine the strength of technical controls, and communicating with staff concerning the effectiveness of administrative, physical, and technical security controls. Information systems may yield information via testing tools and system logs.

One issue the Covered Entity will need to consider is whether it should conduct some kind of penetration testing (using trusted personnel to simulate an attempt to gain unauthorized access to ePHI to test the effectiveness of security controls). If reasonable and appropriate, the Covered Entity should undertake such testing. If the Covered Entity is conducting some kind of penetration testing, it should decide how to conduct the tests. It may decide on manual penetration testing by trained personnel, which involves the expense of hiring people to carry on the testing. Alternatively, the Covered Entity may be able to make use of automated tools to conduct testing. Automated tools may involve an upfront expense of licensing the technology to conduct the testing, but ultimately may involve cost savings. The Covered Entity could also implement some combination of manual and automated testing.

Once the Covered Entity gathers and generates information from the assessment, it should analyze the results to determine if it reveals any weaknesses or vulnerabilities. Vulnerabilities may arise from the absence of a safeguard that should be in place or a weakness in a safeguard. Following the identification of vulnerabilities, the Covered Entity should develop a plan to implement any needed or recommended corrective actions.

The Covered Entity should document the process of its assessment, its analysis of the results, and plan for taking corrective actions. The Covered Entity should then circulate the documentation to key personnel to communicate the results. Since test results reveal vulnerabilities that attackers could exploit, the Covered Entity should also protect assessment results from unauthorized disclosure.

Finally, the Covered Entity should develop and implement a policy regarding repeating security assessment at designated time intervals. Periodic testing will enable the Covered Entity to ensure that changes in the Covered Entity and its information systems do not degrade the level of its security. In addition, assessment outside the normal cycle of testing may become necessary if emergent new threats appear or if the Covered Entity has made significant changes to its operating environment. Likewise, a new or special assessment may become necessary if amendments to the Security Rule or the creation or amendments of other federal or state health care security laws create new or different requirements.

9. Imposing Security Requirements on Business Associates—Section 164.308(b)

(a) Business Associate Contracts and Other Arrangements (Standard)—Section 164.308(b)(1)

A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

This provision requires that the Covered Entity have, from each business associate needing ePHI access, formal assurances in a business associate contract (or equivalent documentation) that the business associate has appropriate security safeguards for ePHI. A Covered Entity must identify which entities are, in fact, business associates with access to ePHI, and what these entities do for the Covered Entity. The Covered Entity must then ensure that written assurances are in place to flow-down security requirements to each of those business associates.

This section does not itself define what those assurances are or what measures specifically need to be in place. Additionally, the rule does not specify which party must determine whether a safeguard is "appropriate." Nonetheless, this section cross-references Section 164.314(a), which requires that business associate contracts contain provisions imposing security requirements on the business associate. Business associate contracts must require the business associate to implement administrative,

physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI.[32]

More particularly, that section states that the safeguards must protect ePHI "as required by this subpart," which is a reference to the Security Rule as a whole. Accordingly, business associates must be, by contract, held to the same standards as the Covered Entity with respect to the covered functions they perform on behalf of the Covered Entity. To the extent a business associate performs only a subset of covered functions for the Covered Entity, only the Security Rule provisions relating to those functions would apply. Nonetheless, business associate contracts commonly specify the specific safeguards the Covered Entity wants the business associate to implement so as to avoid possible ambiguity concerning what the business associate must do.

Business associate arrangements and documenting the flow-down of security requirements on them by written contract are described in more detail above in Section 4.B.1.

(b) Exceptions to the Business Associate Standard—Section 164.308(b)(2)

This standard does not apply with respect to—

> ***(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.***
>
> ***(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or***
>
> ***(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.***

The exceptions under this section concern the communication of ePHI between entities that do not have a true business associate arrangement.

32. 45 C.F.R. § 164.314(a)(2)(i)(A).

Thus, these exceptions are definitional in nature, rather than based on any rationale grounded in information security practices.

(c) Violations of the Standard—Section 164.308(b)(3)

A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

The rationale for business associate requirements is to flow down Security Rule standards, implementation specifications, and requirements from the Covered Entity to the business associate. If a business associate has a business associate contract with a Covered Entity, but is not a Covered Entity itself, the business associate is not subject to regulation by the Security Rule or oversight by HHS. If such a business associate violates security requirements in its business associate contract, the only way for HHS and the Security Rule to redress the violation is through the indirect approach of requiring the Covered Entity to terminate the contract (or at least report the business associate to HHS).[33]

By contrast, this section addresses the situation where the business associate is itself a Covered Entity, and has violated the security requirements in its business associate contract with another Covered Entity. In this situation, the business associate/Covered Entity itself is subject to regulation by the Security Rule and oversight by HHS. This section states that a business associate/Covered Entity in violation of its business associate contract is deemed to be out of compliance with the standards, implementation specifications, and requirements applicable to business associates. Such noncompliance makes the business associate/Covered Entity itself subject to an enforcement action by HHS.

(d) Implementation Specifications: Written Contract or Other Arrangement (Required)—Section 164.308(b)(4)

Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other ar-

33. *Id.* § 164.314(a)(l)(ii). *See also id.* § 164.314(a)(2)(i)(D) (a business associate contract must give the Covered Entity the right to terminate the contract if the business associate does not meet its security obligations under the contract).

rangement with the business associate that meets the applicable requirements of § 164.314(a).

Section 4.B.1 above describes the types of business associate contracts and other written assurances that satisfy the Security Rule. Organizations that procure IT services must ensure that their service providers who process ePHI include in their business associate contracts language that their services comply with all relevant and necessary HIPAA security requirements, standards, and specifications. Aside from written agreements and documentation of the types described in Section 164.314(a), assurances of security may also include service level agreements (SLAs), which IT service providers use to specify their service terms and conditions. See www.itaa.org for a checklist of provisions that may be useful for an SLA.

When the Covered Entity and the business associate are both governmental entities, one possible "other arrangement" for assuring security may consist of a memorandum of understanding that accomplishes the objectives of the business associate agreement. Additionally, where it can be shown that other provisions of applicable law accomplish the objectives of a business associate agreement, a business associate contract is not required. The Covered Entity should retain copies of such applicable law to document the business associate's assurances of security.

10. Conclusion Regarding Administrative Safeguards

The purpose of the Security Rule is to impose reasonable, cost-effective, and appropriate security standards and requirements upon health plans, health care clearinghouses, and health care providers. To establish reasonable, cost-effective, and appropriate policies, procedures, and safeguards, management teams of these Covered Entities must implement administrative safeguards as outlined in this section. A security policy developed following a risk assessment and risk management process forms the initial foundation for administrative controls. Continued diligence enhances the ability of initial policies to keep current with the changing vulnerabilities, threats, and risks.

Management has always been responsible for exercising due care and due diligence in securing business assets. Its responsibilities now include, by regulatory mandate, the protection of ePHI. Security does not stand by itself; it is just one component of good corporate gover-

nance. Therefore, a principal objective of a program to comply with the Security Rule should be coordination with more general security policies and procedures, as well as other compliance efforts.

C. PHYSICAL SAFEGUARDS—SECTION 164.310

> ***Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.***[34]

The physical safeguards section, Section 164.310, consists of four parts: facility access control, workstation use, workstation security, and device and media controls. The subsections below address these four areas.

The definition of "physical safeguards" above implies that the Security Rule addresses two general classes of risks to ePHI: one from natural and environmental causes such as fire, flood, hurricane, and earthquake, and the second from unauthorized human physical access to ePHI. Most of the text in Section 164.310 addresses the threat of unauthorized human access to ePHI. From an information security perspective, however, it is also important to address natural and environmental hazards. The section does have a discussion of contingency operations following an emergency,[35] which would include a natural disaster, but the discussion does not directly address facility construction and operations before a disaster. Planning for fires, floods, hurricanes, earthquakes, and other natural hazards in advance of an event is critical. This is one lesson from Hurricane Katrina.

Facility natural disaster planning is not only good information security practice, such planning is also arguably required by HIPAA and the Security Rule. Section 164.310 does not expressly address facility natural disaster planning the way it does facility security planning for unauthorized human access.[36] Nevertheless, HIPAA requires that Covered Entities maintain "administrative, technical, and physical safeguards" to protect health information.[37] Moreover, the above definition

34. 45 C.F.R. § 164.304 (definition of "physical safeguards").
35. *Id.* § 164.310(a)(2)(i). *See* Section 5.C.1.b.i *infra*.
36. *Id.* § 164.310(a)(2)(ii). *See* Section 5.C.l.b.ii *infra.*
37. 42 U.S.C. § 1320d-2(d)(2).

of "physical safeguards" includes protection of "information systems and related buildings and equipment" and specifically protection from "natural and environmental hazards."[38] Consequently, these two provisions imply that Covered Entities must plan their facilities to address natural disasters and environmental hazards, in addition to man-made threats.

Safeguards to mitigate ePHI security risks due to natural and environmental causes can include:

- Judicious site selection for a data center or other facility housing ePHI;
- Facility construction techniques, including conformance to applicable building codes;
- Fire prevention, detection, and suppression within the facility;
- Flood control or other water management measures within the facility; and
- Regulated and backup air conditioning and power.

1. Facility Access—Section 164.310(a)

(a) Facility Access Controls (Standard)—Section 164.310(a)(1)

Implement policies and procedures to limit physical access to the electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

The facility access controls standard establishes a general requirement of physical access control for the physical location in which ePHI is gathered, stored, processed, and communicated. As mentioned above, facilities planning is an important component of physical security. This section and Section 164.310(a)(2)(ii) address the threat of unauthorized human access to ePHI.

Safeguards to mitigate ePHI security risks due to unauthorized physical human access to the facility include:

- Doors, locks, secure rooms that enforce physical access controls, letting authorized people into the facility, and keeping out unauthorized people or those without a specific need to access a facility;

38. 45 C.F.R. § 164.304 (definition of "physical safeguards").

- Fences and gates that mediate access to the Covered Entities site and buildings;
- Oversight by the use of guards and other security personnel;
- Within rooms, segregating sensitive items or equipment via lockers, cages, and safes;
- Lighting in and around parking lots, hallways, etc.;
- Alarms, cameras, and intrusion detection; and
- Anti-terrorism safeguards.

These safeguards and safeguards against natural and environmental hazards generally represent good business practices, and the Covered Entity may already be in compliance with the physical security portions of the Security Rule. Otherwise, compliance might require remediation in one or more of the areas above, commensurate with the determined risk to ePHI confidentiality, integrity, and availability and appropriate for the size of the Covered Entity. The risk assessment conducted by the Covered Entity[39] should include an analysis of any vulnerabilities stemming from physical threats to the Covered Entity's facility. Risk management principles[40] then can guide the Covered Entity in determining which physical safeguards to implement or strengthen.

Policies on physical access to an information system should also include safeguards to prevent incidental, unauthorized access to ePHI. For example, one kind of vulnerability stems from a physical layout of the facility permitting unnecessarily visible or accessible monitors and keyboards that could expose ePHI to casual observers or tampering. Establishing the location of workstations and plans to prevent incidental access should begin in planning the general layout of the facility.

In considering the scope of physical safeguards for "electronic information systems," Covered Entities should address a crucial issue of scope: what is an electronic information system? While the Security Rule does not define this term, certainly a data center or desktop workstation in an office building, hospital, medical office, laboratory, or other facility qualifies as one. Laptops are computers and perform the same functions as desktop computers, so they too need to be considered electronic information systems. However, mobile devices, such as employee personal digital assistants (PDAs), digital cameras, and

39. *See* Section 5.B.1.a *supra.*
40. *See* Section 5.B.1.b *supra.*

Web-enabled smart cell phones, can capture, store, communicate, or print ePHI. These capabilities suggest that these mobile devices, too, are "electronic information systems." Mobile devices are likely to be deemed "electronic information systems" requiring physical safeguards if the Covered Entity uses them to process or store ePHI.

Physical security also poses a related scope question: what is a facility? The Security Rule defines it as follows: "Facility means the physical premises and the interior and exterior of a building(s)."[41]

"Facility" generally means the building that houses electronic data processing equipment, such as a health care provider's place of business. Although nothing in the rule addresses the issue of mobile information systems, the physical premises, interior, and exterior of a building that contains ePHI could conceivably include an employee's home, an airport, hotel, or other structure outside the general intuitive meaning of a workplace building. Thus, the concept of a regulated facility may extend into these nontraditional areas, and the Covered Entity should develop and implement policies on the allowable use of its information systems outside its ordinary physical premises.

In general, the Covered Entity should develop and then implement reasonable and appropriate physical security policies and procedures. While the HIPAA Security Rule does not specify standards on how to develop and implement policies and procedures, the Covered Entity should use some reasonable and appropriate process that periodically reviews, updates, and checks its physical security. An example of the process might be something like the following:

- Analysis of the current Covered Entity's environment for vulnerabilities and determination of the physical security "gap" that needs to be filled (Review);
- Identification, development, and updating of the policies and procedures to fill the gap (Update);
- Implementation of the policies and procedures to put them into practice (Implement); and
- Testing and validation of the identified updated policies and procedures to ensure they fill the gap identified in Review (Check).

41. 45 C.F.R § 164.304 (definition of "facility").

(b) Facility Access Controls Implementation Specifications—Section 164.310(a)(2)

In addressing facility physical access control safeguards, the rule requires the Covered Entity to address contingency operations, facility security planning, access control and validation, and maintenance record keeping.

(i) Contingency Operations (Addressable)—Section 164.310(a)(2)(i)

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.

This subsection addresses disaster recovery and business continuity concerns first discussed in Section 5.B.7 above. It focuses on the recovery of data and operations following an emergency. Section 164.308(a)(7) of the Security Rule (Contingency Plan)[42] requires the Covered Entity to have a written disaster recovery plan and procedure to continue operations during an emergency or after a disaster. The physical safeguards relative to this plan would include the logistics of responding to a failure of the facility, equipment, or critical service (e.g., power, Internet, or telecommunications).

This subsection raises the following questions when normal controls and procedures are inoperable:

- Who will have access to the primary and any backup facilities during an emergency?
- How will those authorized people gain access to these facilities?
- How will unauthorized people be denied access to these facilities?

The covered entity must, if reasonable and appropriate, implement access control procedures addressing these issues following an emergency. In other words, this addressable implementation specification calls for the Covered Entity to analyze the risk of delay in system restoration (e.g., personnel responsible for recovery are locked

42. This section is discussed in Section 5.B.7 *supra*.

out of physical facilities) caused by efforts to prevent unauthorized persons from compromising system security during disaster recovery procedures. Also, any facilities used specifically for contingency operations to gather, process, store, and transmit ePHI following an emergency should have physical safeguards providing equivalent levels of assurances as those in the Covered Entity's primary facility.

(ii) Facility Security Planning (Addressable)—Section 164.310(a)(2)(ii)

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

The Covered Entity must, if reasonable and appropriate, document and implement procedures that dictate actions that assist in protecting against unauthorized physical access, tampering, and theft of any equipment that contains ePHI. The Covered Entity may find it reasonable and appropriate to include in these policies and procedures the physical security controls described in Section 5.C.1.a above. In addition, policies and procedures should include:

- Who has site and system access and under what conditions;
- Who is responsible for implementing physical security policies and procedures;
- Controls for unauthorized persons, and people with limited authorization (such as visitors, contractors, etc.);
- Property inventory, removal, and tracking of information systems assets (how property and equipment can enter and leave the facility, and for what purposes); and
- Designation of employee responsibility for property while in his/her care outside of the facility.

Procedures need to be in place that document how Covered Entities will strive to prevent equipment and information access, tampering, and theft. These procedures implement the above policy and could include:

- Visitor and contractor access, sign-in/-out logs, escort procedures, restricted areas, etc.;
- Property removal authorization and tracking systems and procedures;

- Physical access control methods such as security badge or card key access systems;
- Issuances of keys and locks to authorized individuals.

Facility security planning is too broad to be comprehensively addressed here. Established businesses of ten or more employees should already have a plan that documents the above safeguards. Covered Entities that do not have a comprehensive facility security plan should create one that complies with the facility access controls standard.

(iii) Access Control and Validation (Addressable)—Section 164.310(a)(2)(iii)

Implement procedures to control and validate a person's access to facilities based on [the person's] role or function, including visitor control, and control of access to software programs for testing and revision.

Covered Entities must implement procedures that restrict access based on personnel rules or functions, if such procedures are reasonable and appropriate. The rule calls for the use of "roles," or groupings of individuals with similar job responsibilities or access requirements, which the Covered Entity assigns to individuals based upon their legitimate job-related facility access requirements and its access control policy. For example, an exterior landscaper probably does not need, and should not have, access to offices with desktops that display patient information. The Covered Entity's policy and procedure should limit the landscaper's facility access to only those areas required for performance of his or her duties. A document that defines the roles used as the basis for granting access to areas where ePHI is available in the facility should include procedures that:

- Sufficiently identify and authenticate individuals before assigning them to their role(s);
- Assign individuals to roles;
- Control access to the facility based upon the individual's role; and
- Verify an individual's identity and role before granting access to restricted areas within the facility.

This subsection specifically calls out the need for procedures that control physical access to software programs for testing and updating, something often overlooked in a facility access control policy and procedure document. The Covered Entity should address how software entry points (open flexible disk drives, tape drives, and other ports on systems that can be used to install and revise software) are secured and who has access to them.

A full discussion of facility access control policy and procedure cannot be presented within the scope of a publication such as this. Publications of the National Institute of Standards and Technologies are useful references for fleshing out the details of physical access controls.[43] Many Covered Entities likely have a plan in which most of the above safeguards have been addressed. If the Covered Entity does not have a comprehensive set of physical access control policies and procedures, the Covered Entity will need one if it is to satisfy this implementation specification.

(iv) Maintenance Records (Addressable)—Section 164.310(a)(2)(iv)

> ***Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).***

Under this implementation specification, the Covered Entity must (if reasonable and appropriate) create and implement policies and procedures to document changes, updates, and repairs to a facility's physical security mechanisms. The Covered Entity should implement:

- A policy mandating the documentation of all repairs to facility physical security mechanisms;
- A policy holding identified personnel responsible for maintaining such documentation;
- A procedure articulating how the organization will produce the documentation; and
- The change-control documentation itself to show ongoing compliance with the policy and procedure.

43. For NIST resources in the computer security area, see NIST Computer Security Division, NIST Computer Security Division's CSRC home page http://csrc.nist.gov/.

The rule appears to apply only to a traditional building facility. Nothing in this section explicitly addresses nontraditional locations, such as an employee's home. Nonetheless, information security policies commonly discuss how employees should physically protect electronic information systems when working from home and while traveling.

2. Workstation Use (Standard)—Section 164.310(b)

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information.

What is a workstation? The Security Rule defines it as follows:

> Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and the electronic media stored in its immediate environment.[44]

"Electronic computing device" is a broad term. Therefore, this definition likely applies to PDAs, mobile phones, and e-mail devices, and their associated removable storage devices to the extent they process or store ePHI. In any case, the Covered Entity should understand what workstations it has and keep track of them, through inventory procedures for instance.

The Covered Entity must prepare policies and procedures on the acceptable use and physical environment of a workstation that stores or uses ePHI. Security considerations include:

- Physical and electronic openness of the environment. For example, can passersby, milling around the office, see a screen containing ePHI?
- Security of remote or off-site locations. The Covered Entity may, for example, wish to prohibit laptop use in a crowded airport, or it may only allow use in a private location such as a hotel room when no one else is around.

44. 45 C.F.R. § 164.304 (definition of "workstation").

These considerations and others may result in a determination that some workstations are not physically secure enough to perform certain functions. These restrictions must be documented by policy and enforced through procedures. Covered Entities should tailor policies and procedures to the capabilities and vulnerabilities of the different types of workstations.

The organization has flexibility to address this requirement as it makes sense to the business while maintaining security of ePHI. At a minimum, the organization should, under this implementation specification, prepare:

- A workstation use policy; and
- A workstation use procedure.

3. Workstation Security (Standard)—Section 164.310(c)

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

The Covered Entity should assess and manage the risk of what work is being done, on what kind of workstations, and where. The Covered Entity must consider the security risks to ePHI before installing a workstation in a particular physical location. For instance, Covered Entities should separate patient waiting areas from workstations to the extent they can in order to prevent viewing ePHI on workstation screens. If possible, workstations can be placed in a separate room. Workstations that need to be near patients, such as in reception areas, should face away from patients. Cubicle and desk designs may enhance separation between workstations and patients. Also, Covered Entities should implement protections against the theft of workstations. Reasonable and appropriate safeguards to protect workstations might include doors, locks, screen-covers, and cable-locks to prevent unauthorized movement of the workstation, as well as cameras and other inventory control and theft-deterrent mechanisms.

Administrative and technical safeguards may be taken into account when a Covered Entity determines the overall risk to ePHI security that a particular location poses. Strong authentication, encryption, and software access controls, for example, *may* mitigate physical security threats. Laptops often contain these kinds of technical safeguards

to mitigate risks to confidentiality. However, if despite the combination of all security safeguards, the physical location of the workstation is insufficiently secure for gathering, processing, storing, or transmitting ePHI, then that workstation should not be used for those purposes at that location.

4. Device and Media Controls—Section 164.310(d)

(a) Device and Media Controls (Standard)—Section 164.310(d)(1)

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

What are electronic media? The Security Rule defines "electronic media" as:

(1) 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
(2) 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.[45]

Because most transmission media (as described above) cannot contain persistent information, this section relies upon definition (1) and primarily governs the movement of information storage devices and media into and out of the facility. Threats that an organization faces include:

- Unknown import and use of a storage device to hold ePHI, which the Covered Entity now would be obliged to manage in accordance with the Security Rule;

45. 45 C.F.R § 160.103 (definition of "electronic media").

- Unknown export of ePHI information onto uncontrolled storage devices connected to workstations, either unintentionally or for purposes of theft. With the popularity and availability of large capacity "thumb drives," users may be able to copy large amounts of ePHI onto these devices and remove them without the Covered Entity's knowledge. The Covered Entity should have acceptable use policies and controls for this kind of storage media;
- Physical removal of media containing ePHI from the Covered Entity's facility;
- Allowing recoverable residual ePHI information to remain on reused, transferred, sold, or otherwise disposed-of electronic media or storage device/devices, including backup media, primary disk storage, semiconductor storage, or any ePHI storage device; and
- Accidental disclosure of ePHI by using electronic storage media for multiple purposes.

To cover these and other security threats, the Covered Entity must develop written policies and procedures covering four specification areas: disposal, media re-use, accountability, and data backup and storage. The first two of these are required, while the others are addressable.

(b) Device and Media Controls Implementation Specifications—Section 164.310(d)(2)

(i) Disposal (Required)—Section 164.310(d)(2)(i)

Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

The Covered Entity must have policies and procedures to ensure ePHI cannot be inadvertently disclosed during or after disposal or re-use of its storage media. To prevent ePHI disclosure during or after storage media disposal, the Covered Entity can:

- Securely destroy the storage media. When erasure is impractical, as in the case of a CD-ROM, the Covered Entity must physically destroy the electronic media.
- Securely erase the ePHI from the storage media using appropriate software or demagnatizing (degaussing) equipment.

One particular threat is the reuse or disposal of a workstation or laptop that previously stored or processed ePHI. Simple file deletion generally does not permanently erase the information, and many utilities can easily recover these files. The Covered Entity must use a secure data destruction methodology to cleanse any storage media before reusing or disposing of them. They should also instruct personnel concerning the threat posed by discarded media and the practices it follows to eliminate ePHI from media before discarding.

(ii) Media Re-Use (Required)—Section 164.310(d)(2)(ii)

> ***Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.***

Covered Entities must address the re-use of media. Reusable electronic media such as disk drives, thumb drives, tape media, Zip drives and other high-capacity disks, rewritable CDs, etc. that have had ePHI recorded on them, must be securely and completely erased to protect against unauthorized disclosure of ePHI when the media are reused. Safeguards to prevent disclosure should account for reasonably anticipated techniques for recovering erased data, such as unerase utilities, block read utilities, etc.

As mentioned above, secure deletion programs are an example of safeguards to facilitate the removal of ePHI from media before they are reused. Covered Entities should train their personnel concerning the vulnerability to disclosure of ePHI from media re-use, as well as the safeguards implemented by the Covered Entity to minimize unauthorized disclosure of ePHI stemming from media re-use. Note, however, that it may be more cost-effective to destroy the storage media than to reuse them.

(iii) Accountability (Addressable)—Section 164.310(d)(2)(iii)

> ***Maintain a record of the movements of hardware and electronic media and any person responsible therefore.***[46]

Where reasonable and appropriate, physical safeguards must include maintaining a record (manual or automated) of all hardware and elec-

46. It appears that the word "therefore" is a typographical error and should actually be "therefor."

tronic media movements, including disposal and reuse, within the organization and outside it, and the individual or group responsible for that movement. Procedural controls (e.g., an inventory) and technical controls can help to monitor media movement. With the introduction of small, removable storage devices such as "thumb drives," users with physical access to standard ports on workstations can move large amounts of information with little, if any record. The Covered Entity should consider this risk and, as a part of its overall security awareness program, train employees in the appropriate and inappropriate use of available storage technology on systems storing ePHI. The intent of this provision is to create strong accountability for protection of ePHI on media circulating within and outside the Covered Entity.

(iv) Data backup and storage (Addressable)—Section 164.310(d)(2)(iv)

Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Data integrity and recoverability are two fundamental goals of the Security Rule. This addressable requirement is intended to prevent accidental data loss from moving equipment, when stored information is at a higher than usual risk of loss. Covered Entities must, before moving equipment containing ePHI, make a backup of the ePHI, if such a procedure is reasonable and appropriate.[47] From a practical perspective, the word "retrievable" in this implementation specification implies that the Covered Entity can also restore the exact copy of the ePHI onto new media. The Covered Entity may make a reasoned, risk-managed decision on how to comply with this specification.

5. Conclusion Regarding Physical Safeguards

The physical safeguard standards represent long-existing good busi-

47. Presumably, this implementation specification applies only to equipment that is normally stationary, such as servers and desktop computers. Covered Entities must, under Section 164.308(a)(7)(ii)(A), backup ePHI on mobile devices, such as laptops and PDAs, on a regular basis. *See* Section 5.B.7.a *supra*. Nonetheless, it is impractical to back up data every time a mobile device is moved. Thus, it does not appear reasonable or appropriate to apply this implementation specification to the day-to-day movement of mobile devices. Backing up may, however, be appropriate where mobile devices are packed and shipped to another location.

ness practices. Many organizations already have the necessary policies, procedures, and metrics in place to manage physical security in the customary system topology, e.g., a central facility with wired desktop workstations and data centers. For these organizations, little additional work beyond compliance verification is required. Others will have to add missing documentation and implement security procedures. For these Covered Entities, existing security standards and best practices should help them so that they do not have to "reinvent the security wheel." One well-known international standard is ISO 17799, which presents an approach to managing many of the safeguards in the rule.

With increasing mobility comes increasing reliance upon the individual to care for his/her workstation. Commodity devices, such as cell phones, cameras, PDAs, laptop computers, and other electronic marvels, increasingly store and process ePHI. Users of these devices must commit to provide acceptable physical security, to use their devices responsibly and securely, and to invoke sufficient technology expertise to protect ePHI should their devices fall into the wrong hands.

With mobility, the definition of "facility" may change to include an employee's home or car, a common carrier, or other building or transportation vehicle. While the Security Rule does not yet expressly cover these alternate types of "facilities," the Covered Entity is still responsible for ePHI physical security without regard to where that information resides. Managing this risk will be a challenge for regulators, Covered Entity management, and information systems users alike.

D. TECHNICAL SAFEGUARDS—SECTION 164.312

This section presents technical requirements with which operators of information systems that store, process, or transmit ePHI must comply. How operators comply with these rules, however, is usually *un*specified, so the Covered Entity must use risk management and business management judgment to satisfy the requirements.

> ***Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.***[48]

48. 45 C.F.R. § 164.304 (definition of "technical safeguards").

Technical safeguards are broken down into two major categories:

1. System security safeguards, which apply to the operation of information systems that store or process ePHI. Operators must configure and maintain their systems using:
   - Access controls;
   - Audit controls;
   - Data integrity assurance; and
   - Person (user) or entity identification and authentication mechanisms.
2. Data transmission security safeguards, which protect information while it is in transit (that is, while moving on the corporate network, an intranet, an extranet, and/or the Internet) between information systems. These safeguards protect information's confidentiality and integrity while it travels between systems.

The Security Rule's technical safeguards section does not specify any technical solution. Rather, it gives the Covered Entity choice and flexibility to meet the requirements.

For more information concerning access control, integrity, authentication, and encryption, readers should consult the Section of Science and Technology Law's previous publications in this area:

- INFORMATION SECURITY COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, DIGITAL SIGNATURE GUIDELINES (1996).
- INFORMATION SECURITY COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, PUBLIC KEY INFRASTRUCTURE GUIDELINES (2003).
- KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL BUSINESS, AND TECHNICAL HANDBOOK (2004).
- PRIVACY AND COMPUTER CRIME COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, INTERNATIONAL GUIDE TO CYBER SECURITY (2004).
- PRIVACY AND COMPUTER CRIME COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, ROADMAP TO AN ENTERPRISE SECURITY PROGRAM (2005).

1. Access Control Safeguards—Section 164.312(a)

(a) Access Control (Standard)—Section 164.312(a)(1)

Implement technical policies and procedures for electronic information systems that maintain electronic protected health

information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

Access controls:

- Allow the right (authorized) people and processes to have access to ePHI in a manner that complies with administrative policy and procedure; and
- Prevent the wrong (unauthorized) people and processes from accessing ePHI.

The analysis described in Sections 5.B.3 and 5.B.4 above describe the process by which a Covered Entity determines appropriate access rights for personnel: who has a need to access which kinds of ePHI, by what means should personnel gain access to ePHI, and what are the minimum access rights necessary for personnel to perform required job duties. The Covered Entity must memorialize its access control practices in policies and procedures. These access control policies and procedures then inform the implementation of policies and procedures for implementing technical safeguards for access control. In any case, the Covered Entity should include in its training program both administrative and technical access control policies and procedures. The Covered Entity should update and improve these policies and procedures based on its experience in implementing them.

The Covered Entity's access control system must identify, authenticate, and authorize people and processes; implement a method of mediating access to information based upon the authenticated entity's authorization; and log information accesses to track user activity upon later review. The Covered Entity must prepare policies and procedures on how it manages and controls access to ePHI. These policies and procedures must meet the following specifications:

- Every user is uniquely identified and tracked.
- User activity is logged and tied to a unique user.[49]
- Access controls are in place and are effective (e.g., ePHI is kept secure from unauthorized access and/or encrypted to ensure its confidentiality).

49. *See also* Section 5.D.2 *infra*.

The following subsections specify the implementation specifications to achieve these access control objectives.

(b) Access Control Implementation Specifications—Section 164.312(a)(2)

(i) Unique User Identification (Required)—Section 164.312(a)(2)(i)

Assign a unique name and/or number for identifying and tracking user identity.

The system must uniquely identify each user and track the user's activities while logged on to the system. No two users may share the same log-on ID or other authentication mechanism to access ePHI. Users sharing credentials might blame each other for unauthorized activity and thereby impede the Covered Entity from holding the wrongdoer responsible for the activity. Thus, this requirement creates user accountability when it is used in conjunction with access controls and an audit trail. This requirement may significantly impact those Covered Entities that have multiple systems, each with shared IDs.[50]

(ii) Emergency Access Procedure (Required)—Section 164.312(a)(2)(ii)

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

This requirement has two parts. The first is a technical requirement for systems to be able to bypass predefined access controls to allow access to ePHI during an emergency, such as when an attending physician needs immediate access to patient information during a health care emergency. The information system must provide a mechanism to do this. Nonetheless, controls should be in place to ensure that emergency procedures are not used to obtain unauthorized access or access control rights.

The second part requires a contingency data access method to be invoked during times of natural or manmade disaster when the information system itself is unavailable, such as due to an electrical power or telecommunications failure.

---

50. UNIX systems, for example, with the standard UNIX "root" administrative account may require additional policy, procedure, and technology to allow multiple system administrators to manage the system without having to share the single "root" account.

In both of these cases the audit system, discussed below, must log the emergency access.

(iii) Automatic Log-off (Addressable)—Section 164.312(a)(2)(iii)

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

The Covered Entity must address how it manages the security risk of logged-in users leaving their workstations unattended, where reasonable and appropriate. This specification calls for a technical safeguard to address situations in which a session is unattended. The safeguard would either terminate or suspend the session after a set time of inactivity.

The Covered Entity should determine a reasonable and appropriate time period of inactivity that would trigger suspension or termination. This inactivity time should then be documented in access control polices and implemented in system administration procedures. System administrators can configure most modern operating systems and applications to set a policy to suspend or terminate a session after a period of user inactivity.

(iv) Encryption and Decryption (Addressable)—Section 164.312(a)(2)(iv)

Implement a mechanism to encrypt and decrypt electronic protected health information.

Covered Entities must encrypt ePHI, if encryption is reasonable and appropriate. This implementation specification applies to ePHI residing on system storage such as disks, tapes, CD-ROMs, flexible disks, etc. The Covered Entity must assess the security risk of ePHI stored in "cleartext" (i.e., unencrypted) on these storage media. Likewise, the specification applies to ePHI in transit from one machine to another. The Covered Entity must also assess the risk of interception of ePHI that it transmits.

If these risks are unacceptably high, and no equivalent alternative measures would provide commensurate security, then the Covered Entity must encrypt stored and/or transmitted ePHI. For example, a Covered Entity might consider whether laptop-stored ePHI should be encrypted on disk when the laptop leaves a secure facility.

If the security risks are acceptably low, or if equivalent alternative measures are available, then the Covered Entity does not need to encrypt stored and/or transmitted ePHI. The Covered Entity may consider all environmental conditions and security measures—administrative, physical, and technical—in assessing these data security risks. Whether or not the Covered Entity encrypts ePHI or uses equivalent alternative measures, it should document its reasoning.

2. Audit Controls (Standard)—Section 164.312(b)

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

While the Security Rule requires audit controls, it does not specify what form they should take or how much audit data is enough. The Covered Entity must have a technical method for logging user activity and a method, automated or procedural, for examining that activity log for unauthorized activity. The overall intent of this requirement is to give the Covered Entity a means of monitoring user access to ePHI and to hold users accountable for their access behavior. Audit information may also be useful evidence in legal proceedings in the wake of wrongful conduct.

The Covered Entity should determine how much audit information it needs to collect and the mechanisms by which it will collect the information. It should also ascertain how it should review log information and how frequently reviews will take place. The Covered Entity's risk analysis should inform it as to areas in which logging is necessary or desirable and the frequency of review. The Covered Entity should then document its audit information gathering and assessment policies and procedures, and train its workforce on its audit program. These policies and procedures should dovetail with the Covered Entity's policies concerning periodic security assessments.[51]

3. Integrity

(a) Integrity (Standard)—Section 164.312(c)(1)

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

51. *See* Section 5.B.8 *supra*.

This standard requires the Covered Entity to consider what kind of technology it should apply to prevent improper data alteration (i.e., protect data integrity) and prevent its alteration or destruction from causes such as:

- Equipment failure
- User accidents or other unintentional acts of authorized users
- Malicious acts of authorized and unauthorized users
- Intruder (hacker) attacks

The Covered Entity's risk assessment[52] should help it determine what risks and vulnerabilities associated with ePHI integrity it should address through integrity safeguards. Integrity vulnerabilities may arise from attackers seeking to alter or corrupt information. In addition, however, the risk assessment may also reveal inadvertent sources of alteration or corruption.

Technologies like redundant arrays of inexpensive disk (RAID), error-correcting memory, and fault tolerant (clustered systems) can reduce risk of data alteration or loss from equipment failure. Well-designed user interfaces to databases and applications can reduce accidental data alteration or loss. Digital signature technology[53] can provide strong assurances of security in identifying corruption or malicious user data manipulation. If the digital signature on information cannot be verified, the receiving party knows that the information is unreliable and may have been altered. Thus, an unverifiable digital signature flags the recipient not to use or rely on unreliable information. The use of checksums[54] also can identify corrupted or maliciously

52. *See* Section 5.B.1.a *supra*.
53. Digital signatures are secure electronic signatures created using certain encryption technology. For more information about how digital signatures work, see INFORMATION SECURITY COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, PUBLIC KEY INFRASTRUCTURE GUIDELINES 304-13 (2003).
54. A checksum is a value associated with data and communicated with the data to the recipient. The sender and recipient use the same method of generating the checksum from the data. If the recipient sees that the checksum transmitted by the sender with the data and the checksum value generated by the recipient are the same, the recipient has some assurance that the information was not altered in transit. The methods of generating checksums range in the levels of assurance provided to detect corruption and malicious alteration of transmitted information.

altered information. The standard does not specify what, if any, technologies are required. These choices are left to the Covered Entity.

In addition to data at rest, this section also covers data in transit. Accordingly, this section overlaps with the integrity controls implementation specification below in Section 5.D.5.b.i.[55]

In any case, technologies exist to reduce risks to data integrity. Therefore, the Covered Entity must define policies and procedures concerning the use of technology to provide assurances of data integrity. The Covered Entity should then communicate its policies and procedures to users, for instance, in the course of its training programs. Finally, the Covered Entity must also reassess its policies and procedures for integrity from time to time in order to account for its experience in implementing them and for changes in its operating environment.

(b) Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information (Addressable)—Section 164.312(c)(2)

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Once a Covered Entity has established its policies and procedures, it must (if reasonable and appropriate) implement the chosen technical approach toward providing assurances of data integrity. Technologies to provide assurances of integrity include the technical solutions mentioned in the previous section. Covered Entities may find it reasonable and appropriate to adopt several technologies that meet the objective of maintaining ePHI integrity in the Covered Entity's information system.

4. Person or Entity Authentication (Standard)—Section 164.312(d)

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

This provision requires that systems technically verify that the users or devices accessing ePHI are who they indicate they are. Section 5.B.4

55. 45 C.F.R. § 164.312(e)(2)(i).

above concerns the administrative process of granting, exercising, and updating access privileges: who should have access to what kinds of ePHI under what circumstances. Also, Section 5.B.4 describes the authentication process and the threats it addresses: ensuring a real-world identity exists for an authorized user, and ensuring that a person seeking ePHI access is, in fact, the authorized user. By contrast, this section concerns the technical mechanisms to enforce access control policies and procedures via authentication. For instance, technical controls can ensure that a person seeking to log on to a system is, in fact, the authorized user he or she purports to be.

A Covered Entity's risk assessment[56] should determine how vulnerable its systems are to impersonation by unauthorized personnel seeking access to ePHI. The risk assessment should also suggest mechanisms for safeguarding against impersonation. Authentication is a key challenge in electronic communications, especially through the Internet, because communicating parties cannot use authentication methods available in a face-to-face setting, such as checking photo identification documents.

Systems commonly use passwords, tokens, biometrics, or dial-back techniques to verify an individual's or entity's identity. The Security Rule requires that the system verify identity; it does not specify any specific technology for doing so. Sometimes, authentication mechanisms are referred to as "factors" or authentication approaches:

- One kind of authentication relies on something that the user knows, such as a password or PIN. As long as the user, and only the user, knows the password, entering the password confirms that the user is who he or she claims to be.
- Another kind of authentication is based on something that the user possesses, such as a card with a magnetic stripe,[57] smart card, or other kind of physical token. The user allows the system to read the information on the token (e.g., by inserting it into a reader). As long as the user has not lost the token, using the token proves the user's identity.
- Finally, biometric identifiers, such as fingerprints, iris patterns, and voice patterns, can authenticate a user. A device reads the

56. *See* Section 5.B.1.a *supra*.
57. In financial services, for example, an example of a card with a magnetic stripe is the ATM card.

user's fingerprint or other identifier to ensure that it matches the identifier stored in its system. As long as the identifier is unique to the user, it shows the user's identity.

Digital signatures supported by a "public key infrastructure" (PKI) can also serve to authenticate users. Digital signatures are a secure form of electronic signature making use of particular cryptographic techniques to provide assurances, for instance, that a signature has originated from an identified person. PKIs frequently make use of "digital certificates," which can serve, among other things, as electronic credentials to identify a user. The use of passwords, tokens, and biometric readers can enhance the security of a PKI authentication mechanism and provide relatively high assurances of identity of known users.[58]

The Covered Entity's risk assessment should determine whether using one of the above factors or approaches is reasonable and appropriate, or whether more than one factor is needed to provide adequate authentication. The combination of a user name and password has been considered sufficient for many lower security applications. By contrast, higher security applications generally call for two-factor authentication. The risk assessment should account for the trade-off between the rigor provided by high security authentication mechanisms and the increased cost and difficulty associated with their use.

Regardless of the authentication mechanism chosen, the Covered Entity should train its personnel in the secure method of using the authentication mechanism. Training topics include secure establishment of the mechanism, preventing compromise, and notifying the appropriate security personnel if a mechanism is compromised. For instance, if the Covered Entity uses passwords, it should instruct users about choosing strong passwords, methods of avoiding compromise of the password, and how to notify the appropriate personnel in case the password is compromised.[59] The Covered Entity should assess the effectiveness of its authentication mechanism and adjust its policies, procedures, and authentication methods as it obtains experience in controlling access to ePHI and as its operating environment changes.

---

58. For a tutorial on how digital signatures work, see INFORMATION SECURITY COMMITTEE, ABA SECTION OF SCIENCE AND TECHNOLOGY LAW, PUBLIC KEY INFRASTRUCTURE GUIDELINES 304-13 (2003).
59. *See* Section 5.B.5.d *supra*.

5. Transmission Security—Section 164.312(e)

(a) Transmission Security (Standard)—Section 164.312(e)(1)

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

This section and the subsections below apply to information while in transit over a network such as the Internet or an internal network. Security threats addressed include:

- Eavesdropping: an unauthorized person "listens" in on an unprotected or open network carrying ePHI; and
- Data modification: interception and surreptitious modification of ePHI by an intruder in a way that the recipient cannot detect.

As with other technical mechanisms, the Covered Entity's risk assessment[60] should inform the Covered Entity as to the various threats that may affect transmitted ePHI and possible mechanisms that may provide security to address the threat. The Covered Entity must protect data while in transit using mechanisms providing a level of security that is commensurate with the transmission security risks and their associated mitigation costs.

Once the Covered Entity develops policies and procedures for the use of specific technical safeguards for transmission security, the Covered Entity should implement them and train its personnel on their proper use. It should also monitor the use of these safeguards to determine their effectiveness. This experience along with changes in risks and threats facing the Covered Entity should provide feedback for changes and updates in the Covered Entity's policies and procedures.

One commonly used technical standard for transmission security is secure sockets layer (SSL). SSL protects information in transit from interception via encryption. Also, SSL includes the use of a checksum[61] to ensure the integrity of the message. Finally, SSL makes use of digital certificates to provide assurances of identity concerning the server with

60. *See* Section 5.B.1.a *supra*.
61. For information concerning checksums, see Section 5.D.3 *supra*.

which the user is communicating, and optionally to authenticate the user to the server.[62]

(b) Transmission Security Implementation Specifications—Section 164.312(e)(2)

(i) Integrity Controls (Addressable)—Section 164.312(e)(2)(i)

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Under the standard in Section 164.312(c)(1) the Covered Entity must address what technology it will use to ensure ePHI is not undetectably changed, altered or destroyed.[63] In implementing this standard, under Section 164.312(c)(2), Covered Entities may implement certain technologies to provide assurances of integrity.[64] This section focuses on the integrity of ePHI that is in transit from one system to another. Because data may pass through systems outside of its control, the Covered Entity cannot ensure that ePHI will arrive at destinations unchanged. It can ensure, though, that the recipient can detect any changes or data loss during transmission. Presumably, the recipient can, upon detection of modification or loss, request a retransmission. Under this section, where reasonable and appropriate, Covered Entities must use the technologies described in Section 5.D.3 above to ensure the integrity or detect alteration of ePHI in transit.

(ii) Encryption (Addressable)—Section 164.312(e)(2)(ii)

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

---

62. For instance, in the ecommerce context, SSL protects sessions in which a user purchases products from an online merchant's so-called "secure site." SSL authenticates the merchant to the user's browser, so that the user knows the identity of the merchant whose site he or she has accessed. Also, integrity checks provide protection against corruption of the data being communicated. Finally, SSL involves encryption of the session to prevent interception of sensitive information, such as credit card information. SSL can provide these same capabilities in the context of the transmission of ePHI.
63. *See* Section 5.D.3.a *supra*.
64. *See* Section 5.D.3.b *supra*.

Under Section 164.312(a)(2)(iv), Covered Entities may need to implement a mechanism to encrypt ePHI.[65] This section focuses on encryption for ePHI being transmitted from one system to another. The Covered Entity must evaluate and decide whether encrypting some or all of its ePHI transmitted over networks is reasonable and appropriate. If encryption is reasonable and appropriate, the Covered Entity must implement encryption technology. Considerations going into this decision include:

- The recipients' ability to receive and decrypt an encrypted message;
- The sensitivity of the transmitted information;
- The potential impacts of unauthorized ePHI disclosure;
- The costs of implementing, managing, and operating the encryption system; and
- The vulnerabilities of the network and overall environment.

This analysis applies to ePHI without regard to its particular method or protocol of transmission. Therefore, transmissions such as e-mail, Web, and dedicated protocol traffic may all need to be encrypted, depending on the extent to which encryption is reasonable and appropriate for the Covered Entity.

6. Conclusion Regarding Technical Safeguards

The HIPAA technical safeguards are intended to be met with reasonable, appropriate, and cost-effective measures to ensure the security of ePHI. Compliance with the rule will include:

- A full assessment of current ePHI security and protection practices
- A reasoned security response commensurate with the discovered security risks
- Cost-effectiveness
- Achievability with available technology
- Consistency with generally accepted sound information technology systems management and security philosophy
- Likely influence on future technology purchases

65. *See* Section 5.D.1.b.iv *supra*.

In many respects, the Security Rule represents sound business and information technology systems management practices that health care and other industries have recognized for many years. The Covered Entity may already be complying with most, if not all, provisions of the Security Rule. At the very least, however, the Covered Entity must assess its compliance with the Security Rule to demonstrate to itself, its business partners, auditors, and potentially HHS that it meets ePHI security standards.

HHS intended that generally accessible, commercially available technology would suffice for compliance with the Security Rule. The Covered Entity may already have sufficient IT resources to comply with the technical portion of the Security Rule, and (at least in theory) any missing technology should be available from multiple vendors at reasonable costs. Compliance, however, must be reviewed periodically. As security threats and reasonable and appropriate technology both constantly change, the Covered Entity must reassess its ePHI security risk and technical measures.

E. POLICIES, PROCEDURES, AND DOCUMENTATION—SECTION 164.316

1. Policies and Procedures (Standard)—Section 164.316(a)

> ***Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.***

One of the key components of any security program is documentation. The various sections of the HIPAA Security Rule include a requirement that Covered Entities implement "reasonable and appropriate" documentation in the form of policies and procedures to comply with standards and implementation specifications in the regu-

lations.[66] Various sections in the regulations require the implementation of security policies and procedures.

In the development of policies and procedures, Covered Entities should ensure that they are sufficient to cover all of the applicable security criteria. Applicable criteria include the portions of the Security Rule that are mandatory (standards and required implementation specifications) and addressable implementation specifications (or equivalent alternative controls) that reasonably and appropriately apply to the Covered Entity. If the policies and procedures are incomplete or do not cover all of the applicable security criteria, then they will not be sufficient for compliance.

Further, Covered Entities should tailor their policies and procedures to the actual practices of the staff and business associates in conducting their day-to-day activities. Covered Entities that simply copy "off the shelf" policies and procedures from a book or other source risk having policies and procedures that are divorced from the reality of their daily activities. Instead, Covered Entities should use their risk-assessment procedures to develop customized policies and procedures that address their individual situations and the risks they face. The end result should be policies and procedures that create effective and realistic risk-management approaches tied to how Covered Entities really operate.

Also, the scope of the Covered Entity's policies and procedures should account for:

- Its size, complexity, and capabilities;
- Its security capabilities regarding its technical infrastructure, hardware, and software;
- The costs of security measures; and
- The probability and criticality of potential risks to ePHI.[67]

Policies and procedures should lay out security targets that readily permit auditing and other assessment. That is, an assessor should be able to look at a policy or procedure document to check to see whether the Covered Entity actually does what it says it does in the document. Policies and procedures that are insufficiently clear or set out goals that cannot be measured make it difficult to assess compliance.

66. 45 C.F.R. § 164.316(a).
67. *See id.* § 164.306(b).

Finally, Covered Entities should reexamine their policies and procedures on a periodic basis to make sure that they remain reasonable and appropriate. Threats, vulnerabilities to those threats, security technology, information technology, the Covered Entity's operating environment, and business needs change over time. Security incidents may also call attention to needed amendments to policies and procedures. Covered Entities should make amendments as needed to account for these changes. Periodic reexamination and amendment can ensure that policies and procedures remain relevant over time.

When making amendments, Covered Entities should follow the change control procedures set forth in the policies and procedures. For instance, change control procedures can address issues such as:

- Who can propose changes
- Who must approve changes
- Notifications to affected parties
- The process for obtaining approval and finalization
- When documentation becomes effective and when it must be reevaluated

Further, when making changes, Covered Entities should have explanatory documentation, such as the reason for the changes, the nature of the changes, and how they intend to implement the changes. Covered Entities may find it helpful to task a team of personnel to solicit input, investigate changed circumstances, and implement amendments to policies and procedures periodically.

2. Documentation—Section 164.316(b)

(a) Documentation (Standard)—Section 164.316(b)(1)

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Covered Entities must maintain policies and procedures in written form, which may be in the form of electronic records,[68] such as word processing files. Likewise, some of the regulations require that actions, activities, or assessments be documented. For instance, if an implementation specification is not reasonable or appropriate to implement, the Covered Entity must maintain documentation as to why it is not and should document why any equivalent alternative measure would be reasonable and appropriate.[69] If a Covered Entity determines that no alternative measures are reasonable and appropriate, the Covered Entity should document the reasoning behind its decision. Where regulations require documentation, Covered Entities must maintain a written record of the action, activity, or assessment. Again, electronic documents are acceptable.[70]

One consideration is whether the Covered Entity has a general set of security documents, in which HIPAA Security Rule compliance is one component, or whether the Covered Entity maintains a separate set of HIPAA-specific documentation. The regulations do not require one or the other. Therefore, a Covered Entity with a general security policy can simply add HIPAA-specific provisions to its security policy, or it could write a separate HIPAA-specific document to address the HIPAA Security Rule. For Covered Entities that face requirements from multiple sources, such as health insurers, it may be easier to have a single security policy combining mandates from HIPAA, Gramm-Leach-Bliley Act, and other requirements, as opposed to having multiple policies, each addressed to one statute or source. At a minimum, however, HIPAA-specific documentation should not conflict with other security policies and procedures.

(b) Documentation Implementation Specifications—Section 164.316(b)(2)

(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

68. *Id.* § 164.316(b)(1)(i).
69. *Id.* § 164.306(d)(3)(ii)(B).
70. *Id.* § 164.316(b)(1)(ii).

(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Required Implementation Specifications for documentation state that Covered Entities must retain the documentation described above for a period of six years. The six years start to run from the documentation's date of creation or the date when the described program was last in effect, whichever is later.[71] Covered Entities retaining documentation in electronic form over time should consider:

- Measures to ensure that documentation is not inadvertently lost, destroyed, or corrupted.
- Measures to prevent intentional alteration.
- Maintaining backup copies of the documentation to ensure recovery from loss, destruction, corruption, or malicious alteration.
- Accounting for changes in software and hardware and ensuring that archived documentation is still accessible on currently used systems. For instance, if a Covered Entity migrates from the use of one word processing program to another, the Covered Entity may want to retain an old system to access archived word processing documents, or archived documentation may need to be resaved in the new format.

Covered Entities must also make this documentation available to the personnel who are responsible for implementation of the procedures documented.[72] Documentation, such as policies, procedures, and their amendments, would do no good unless the personnel implementing them know where to find them and have access to them. One way to make documentation available is to include it in routine, special, or refresher education and security awareness training.

71. *Id.* § 164.316(b)(2)(i).
72. *Id.* § 164.316(b)(2)(ii).

Finally, Covered Entities must review their documentation from time to time and update it as needed. Updates are required whenever a Covered Entity makes changes in its environment (e.g., its facility) or operations (such as the activities it conducts) that affect the security of ePHI.[73] Good documentation is also crucial in any audit or enforcement situation to demonstrate the organization's good-faith efforts to comply with the rules. HHS has made it clear that such efforts will affect any civil money penalty assessment.[74]

73. *Id.* § 164.316(b)(2)(iii).
74. *See* preamble to interim enforcement rules (45 C.F.R. § 160.500 et seq.), 68 Fed. Reg. 18895, 18897 (Apr. 17, 2003). For a more detailed discussion of civil money penalties, see the discussion in Chapter 7 *infra*.