

**HIPAA'S FINAL SECURITY REGULATIONS FOR ELECTRONIC
PROTECTED HEALTH INFORMATION**

ALI-ABA Video Law Review

Health Plans, HIPAA, and COBRA Update

April 27, 2005

Prepared by:

**Greta E. Cowart, Esq.
Haynes and Boone, LLP
901 Main Street, Suite 3100
Dallas, TX 75202-3789
214-651-5000**

TABLE OF CONTENTS

	Page
I. Overview	1
A. Purpose.....	1
B. Standards.....	1
C. Implementations Specifications	1
D. Impact on Privacy Regulations	2
E. Electronic Protected Health Information Subject to the Final Security Regulation is Required.	2
II. General Requirements	3
A. Basic Requirements	3
B. Who is Subject to the Final Security Regulations.....	3
C. Compliance Has Flexible Standards	3
III. Organizational Standards	4
A. Application of Organizational Standards.....	4
B. Hybrid Entity	4
C. Affiliated Covered Entities	5
D. Group Health Plan	5
E. Addressable Implementation Specifications.....	6
F. Documentation and Record Retention	6
G. Compliance Deadlines	6
IV. Standards and Implementation Specifications	7

I. Overview.

The Final Security Regulations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) were issued on February 20, 2003 at 68 F.R. 8333 (2003) (the “Final Security Regulations”). The Final Security Regulations are effective April 21, 2003 with compliance deadline of April 21, 2005 for group health plans with \$5 million or more in receipts, and in April 21, 2006 with respect to the small health plans. They also apply healthcare providers that transmit claims electronically and healthcare clearing houses effective as of April 21, 2005.

A. Purpose. The purpose of the Final Security Regulation is to insure the integrity, security and availability of electronic health information that is identifiable to an individual. The Final Security Regulation was issued recognizing a balancing act. The Final Security Regulations recognize there must be balancing between the size of the entity and its ability to meet certain standards and the need for security. The Final Security Regulations are designed to require procedures for reasonably anticipated threats or hazards.

B. Standards. The Final Security Regulations have two standards regarding organizational requirements for business associates and for group health plans. The Final Security Regulations also include standards for four types of organizations, these sections are in part borrowed from the sections moved from the Privacy Regulations to the Security Regulations, and in part with a new additional focus. The four types of organizations with provisions moved to and/or augmented in the Security Regulations are health care clearinghouses, health plans, affiliated covered entities and hybrid entities. The Final Security Regulations include eighteen technical standards, two covering authentication or identification policies and procedures, and thirty-six implementation specifications with respect to the various standards. The Final Security Regulations provide for implementation standards that are either “required” or “addressable.” The “addressable” standards require the organization assess whether the implementation is feasible and it is necessary to provide adequate security for its electronic protected health information. The required implementation standards must be met. The Final Security Regulation defines the scope of information protected by the Final Security Regulation as “protected health information in electronic form.” The proposed regulation had applied to “electronic health information pertaining to individuals.”¹

C. Implementation Specifications – Now Required and Addressable. The Final Security Regulations adopt number of standards and implementations specifications that provide instructions for implementing the standards.²

1. Required implementations specifications must be satisfied.
2. The addressable implementation specification must each be assessed. The assessment of each addressable implementation specification must be documented with the rationale for each decision documented. For each addressable implementation specification the covered entity must do one of the following:
 - a. If the addressable implementation specification is determined to be reasonable and appropriate with respect to that covered entity, the covered entity must implement it.

¹ 68 FR 8335 (2003).

² 68 FR 8336 (2003).

b. If the addressable implementation specification is determined to be inapplicable and/or inappropriate and/or an unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an alternative security safeguard, the covered entity may implement an alternate measure that accomplishes the same goal as the addressable implementation specification. The covered entity that meets the standards through an alternative measure must document the decision not to implement the addressable implementation specification, the rationale behind the decision, and the alternative safeguard implemented to meet the standard.

c. A covered entity may also decide that a given implementation specification is simply not applicable (that it is neither reasonable, nor appropriate) to the covered entity's situation and the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. The covered entity in this situation must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met.

d. The covered entity may implement a combination of one or more of the addressable implementation standards and one of the alternative security measures. The decision on whether or not to implement an addressable implementation standard must be made considering the entity's risk analysis, risk mitigation strategy, what security measures are already in place and the costs of the implementation.³

D. Impact on Privacy Regulations. The Final Security Regulations moved a number of definitions from their locations in the final privacy regulation and standards for electronic standard transaction regulations to the Final Security Regulations. The definitions include business associate, covered entity, disclosure, electronic media, electronic protected health information, healthcare, healthcare clearing house, healthcare provider, health information, health plan, individually identifiable health information, implementation specification, organized healthcare arrangement, protected health information, standards, use and workforce. These were removed from their previous locations in the privacy and electronic transaction standard regulations and moved to 45 C.F.R. § 160.103.

New definition section also modified the definition of a number of items. Previously the definition of electronic media was contained in 45 C.F.R. § 162.103, it has now been moved to 45 C.F.R § 160.103 and it was modified to include electronic storage in the electronic media. Thus, both the privacy (subpart E) and security (subpart C) regulations apply to information stored in electronic media as well as information that transmitted in the electronic media.

E. Electronic Protected Health Information Subject to Final Security Regulation is Clarified. The Final Security Regulations further clarified that transmission of information that is not in an electronic form before the transmission is not covered by the definition of electronic media.⁴

The health information covered by the Final Security Regulation is broader than the designated code set covered by the standards for electronic claim transactions regulations and includes telephone voice response, and fax back (that is a request for information from a computer made via voice or telephone keypad input, with a request for information returned as a fax.) Both are under the Final Security Regulation because they are used as input and output devices for computers and not because they have

³ 68 FR 8336 (2003).

⁴ 68 FR 8339 (2003). 45 C.F.R. §160.103 (2003).

computers in them. They are included in the generally required computer protections for only one of the parties involved and not the other. The information transmitted via telephone is non-electronic format while it is being transferred, but it is electronic once it is received. Even though some more recently made electronic devices contain a microprocessor, they are not included in the term “computer” which is intended to include software programmable computers, for example personal computers, minicomputers and mainframes. Copy machines, fax machines and telephones even though they contain memory and can produce multiple copies for multiple people, are not intended to be included in the term computer. Both paper to paper faxes, person to person telephone calls and calls via teleconferencing or messages left on voicemail are not in electronic form before the transmission and those activities are not covered by the Final Security Regulation.⁵ The Final Security Regulation guidance regarding transactions subject to the rule differs from the electronic standard transaction rule’s guidance on what constitutes an electronic transaction with respect to fax back and voice response systems. Those types of electronic media are intended to only be subject to the Final Security Regulations.⁶

II. General Requirements.

A. Basic Requirements. The Final Security Regulations require the covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates receives, maintains or transmits.⁷ The covered entity must protect against any reasonably anticipated threats or hazards to the security or integrity of the electronic protected health information and must protect against any reasonably anticipated uses or disclosures of the electronic protected health information that would not be permitted or required under the Privacy regulations issued at 45 C.F.R. Parts 160 and 164 (the “Privacy Regulations” or “subpart E”). The covered entity must ensure that its workforce complies with the Final Security Regulations.⁸

B. Who is Subject to the Final Security Regulations? A covered entity for purposes of the Final Security Regulations includes a health plan, a health care clearinghouse and a healthcare provider who transmits any health information in electronic form in connection with a transactions covered by the electronic standard transaction regulations⁹ and the Privacy Regulations.¹⁰ A covered entity must comply with the standards and implementation specifications with respect to electronic protected health information.¹¹ Thus, if a covered entity does not transmit or maintain electronic protected health information, it should not be subject to these standards. Furthermore, since the exclusion under the definition of a group health plan for plans with less than 50 participants that are self-administered applies to define a health plan and a covered entity for the security regulations, these small self administered plans also would not be subject to the HIPAA security requirements.¹²

C. Compliance Has Flexible Standards. The Final Security Regulations provide covered entities with the opportunity to use a flexible approach to implementing the standards. The Final Security Regulations are designed to be flexible to allow the covered entity to reasonably and appropriately implement each of the standards and implementations specifications. The covered entity must assess a number of factors when deciding what security measures to use. The covered entity must consider the size, complexity and capabilities of the covered entity, the covered entity’s technical

⁵ 68 FR 8342.

⁶ 68 FR 8343.

⁷ 45 C.F.R. §145.306(a) (2003).

⁸ *Id.*

⁹ 45 C.F.R. Part 162 (2000 as modified on February 20, 2003).

¹⁰ 45 C.F.R. §164.104 (2003).

¹¹ 45 C.F.R. §164.302 (2003).

¹² 45 C.F.R. §160.103 (2000 and 2002).

infrastructure, hardware and software security capabilities, the cost of the security measures and the probability and criticality of potential risk to the electronic protected health information. The Final Security Regulations have standards that must be complied with in five sections, sections 164.308, 164.310, 164.312, 164.314 and 164.316. Under the standards there are implementations specifications. The implementations specifications are either required or addressable. If the implementation specifications is addressable, then the entity must assess whether the specification is reasonable and appropriate as a safeguard in the covered entity's environment when it is analyzed with reference to the likely contribution to protecting the entity's electronic protected health information and implementation specification if it is reasonable and appropriate or if implementing the specification is not reasonable and appropriate, the covered entity must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if the alternative measure is reasonable and appropriate.¹³ Ongoing review is required by the Final Security Regulations which also require that security measures that are implemented to comply with the Final Security Regulations' requirement must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information.¹⁴ The Final Security Regulation then requires a number of administrative safeguards, physical safeguards and technical safeguards are well as business organization requirements that must be met with respect to electronic protected health information ("EPHI"). The Final Security Regulation further requires that there be policies, procedures and documentation.

III. Organizational Standards.

A. Application of Organizational Standards. The organizational standards apply to health care clearinghouses, hybrid entities, health plans and affiliated entities. Some of the standards were originally included in the Final Privacy Regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")¹⁵ have been moved into the Final Security Regulations.

Four organizational standards are brought over from a former privacy regulation by moving provisions contained in the Privacy Regulations into the Final Security Regulations.

B. Hybrid Entity. The final regulations moved the definition of the hybrid entity and the organization requires from the privacy regulations into § 164.103 and § 164.105 of the Final Security Regulations. The Final Security Regulations requirements for a hybrid entity requires it must have healthcare components, must be a covered entity whose business activities included both covered and non-covered functions and it must designate its healthcare components as required under Final Security Regulations.¹⁶ For example, a hybrid entity could be a wrap around welfare benefit plan that includes both health benefits, and life insurance or disability benefits. In order to comply the plan must designate the entities that are healthcare components. The components each must perform a function of the covered entity either as a health plan, healthcare provider or healthcare clearing house as applicable. The hybrid entity must protect the electronic protected health information that creates, receives, maintains or transmits by or in behalf of the healthcare component of the covered entity or hybrid entity.¹⁷

The hybrid entity must insure that the each of the healthcare components safeguards the electronic protected health information and must insure that the healthcare component does not disclose protected

¹³ 45 C.F.R. §164.306(d) (2003).

¹⁴ 45 C.F.R. §164.306(e) (2003).

¹⁵ 45 C.F.R. Parts 160 (May 31, 2002) and 164 (August 14, 2002).

¹⁶ 45 C.F.R. §164.103 (2003).

¹⁷ *Id.*

health information to any other component and circumstances that would violate the privacy regulation if those entities are separate and distinct legal entities. The hybrid entity must make sure that the healthcare components protect the electronic protected health information with respect to any other component of the hybrid entity to the same extent it would required under the Final Security Regulations.¹⁸

The plan make sure that healthcare components that create, receive, maintain or transmit electronic protected health information complies with the Final Security Regulations and does not use or disclose protected health information in any way that would violate the Privacy Regulations. A person who performs duties for both the healthcare component and in the capacity as a member of the workforce as such component and for another component must not use or disclose protected health information that is created or received in the course of or incident to that individuals work for the healthcare component in a way that would violate the Privacy Regulations.¹⁹ The hybrid entity has responsibility for compliance and enforcement with respect to the Privacy Regulations' requirements and implementing policies and procedures to ensured compliance with both the Privacy Regulations and the Final Security Regulations. The hybrid entity must designate the components that are healthcare components within the entity and document such designations. Those entities that are thus so designated must perform covered functions or activities that would make the healthcare component a business associate of a covered entity.²⁰

C. Affiliated Covered Entities. The Final Security Regulations permit legally separate covered entities that are affiliated to designate themselves as a single covered entity. Entities are affiliated if all of the covered entities are under common ownership or control. Ownership or control exists if an entity or entities possess ownership or equity interest of 5% or more in another entity.²¹ If the covered entities designate themselves as a single entity the covered entities must document such designation.²²

The affiliated covered entities must meet certain safeguard requirements and that they must insure that the electronic protected health information that they create, receive, maintain or transmit complies with the Final Security Regulations and that the covered entity's disclosure of protected health information complies with the Privacy Regulations. The affiliated entities must maintain documentation showing their written or electronic record of their designation and they must maintain records for six years from the date the information was created or the date it was last in effect, whichever is later.²³

D. Group Health Plan.

1. Which group health plans must be amended for the Final Security Regulations?
A group health plan must also meet certain standards under the both the Privacy Regulations and Final Security Regulations in addition to the general security standards required by statute of a covered entity, unless it meets one of the exceptions in (a) or (b) below or unless it is not subject to the privacy and/or security regulations as discussed in II.B. above. The only group health plans that are excepted from the additional requirement are group health plans who only disclose electronic protected health information to a plan sponsor either (a) pursuant to a disclosure from the group health plan, health plan issuer or an HMO in the form of summary health information for premium bidding purposes, or (b) when the group health plan insurance issuer or HMO only provide information to the group health plan sponsor on whether an individual is enrolled or dis-

¹⁸ 45 C.F.R. §164.105(a) (2003).

¹⁹ 45 C.F.R. §164.105(a)(2)(ii) (2003).

²⁰ 45 C.F.R. §164.105(a) (2003).

²¹ 45 C.F.R. §164.103 (2003).

²² 45 C.F.R. §164.105(b)(1) (2003).

²³ 45 C.F.R. §164.105(c) (2003).

enrolled or whether they are participating or not participating in any particular group health plan.²⁴

2. **Group Health Plan Document Requirements.** In all situations other than those in D. 1.(a) and (b) above, the group health plans must insure that the plan documents include certain provisions. The provisions that must be included are that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. In order to do this, the plan documents must meet certain requirements which are required implementations specifications under the Final Security Regulations. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement (a) administrative, physical and technical safeguards that will that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains or transmits on behalf of the group health plan; (b) it must insure the adequate separation between the plan and the plan sponsor is supported by reasonable and appropriate security measures; (c) the documents must insure that any agent, including a subcontractor, to whom it provides the information agrees to implement reasonable and appropriate security measures to protect the information (such as in the event of a plan sponsor providing information to a broker seeking renewal bids); and (d) the document must require the plan sponsor to report to the group health plan any security incident of which it becomes aware.²⁵

E. Addressable Implementation Specifications. Each covered entity must implement reasonable and appropriate policies and procedures to comply with the Final Security Regulations standards, implementation specifications and other requirements considering the covered entity's size, complexity and capabilities, the covered entity's technical and infrastructure, hardware and software security capabilities, the cost of the security measures and the probability and criticality of potential risk to electronic protected health information.²⁶ The Final Security Regulations can provide that the covered entity may change its policies and procedures at any time provided the changes are documented and implemented as required under the Final Security Regulations.

F. Documentation and Record Retention. The documentation requirement imposed by the Final Security Regulations is that the covered entity must maintain the policies and procedures implemented to comply with the Final Security Regulations in a written or an electronic written form. If there is an action, activity or assessment that is required by the Final Security Regulations to be documented, the covered entity must maintain a written record of the action, activity or assessment (including electronic records). These records must be maintained for six years from the date the record is created or the date when it was last in effect whichever is later. The documentation that is made by the covered entity must be made available to the persons who are responsible to implement the procedures to which the documentation relates. The covered entity must review the documentation periodically and update it as needed in response to environmental or operational changes that effect the security of the electronic protected health information.²⁷

G. Compliance Deadlines. Every health plan that is not small health plan must comply with the requirements of the Final Security Regulations no later than April 21, 2005. The small health

²⁴ 45 C.F.R. §164.314(b)(1) and §164.504(f)(1)(ii) and (iii) (2003).

²⁵ 45 C.F.R. §164.314(b)(2) (2003).

²⁶ 45 C.F.R. §164.316(a) (2003).

²⁷ 45 C.F.R. §164.316(b) (2003).

plan must comply no later April 21, 2006. Healthcare clearing houses and healthcare providers must comply no later than April 21, 2005.

IV. Implementation Standards and Specifications.

The following charts are based upon the matrixes at the end of the Final Security Regulations and have been augmented to incorporate the guidance included in the preamble to the Final Security Regulations and in the Final Security Regulations themselves.

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
Security Management Process- These are procedures to prevent, detect, contain and correct security violations. ²⁸	164.308(a)(1)	Risk Analysis –An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks or vulnerabilities. ²⁹	(R)	Required- An accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of the electronic protected health information (“EPHI”) held by the covered entity. ³⁰
		Risk Management -Security measures must remain current and must be periodically reassessed and updated as needed. ³¹	(R)	Required- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. ³²
		Sanction Policy	(R)	Required- The covered entity must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures it establishes. ³³
		Information System Activity Review	(R)	Required- The covered entity must establish procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. ³⁴

²⁸ 45 C.F.R. §164.308(a) (2003).

²⁹ 68 F.R. 8346 (2003).

³⁰ 45 C.F.R. §164.308(a)(1)(A) (2003).

³¹ 68 F.R. 8346-8347 (2003).

³² 45 C.F.R. §164.308(a)(1)(B) (2003).

³³ 45 C.F.R. §164.308(a)(1)(C) (2003).

³⁴ 45 C.F.R. §164.308(a)(1)(D) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
Assigned Security Responsibility	164.308(a)(2)		(R)	Required- While there is no implementation specification for this standard, the preamble indicates that a sanction policy is a required implementation specification because the statute required covered entities to have safeguards to ensure compliance by officers and employees, a negative consequence to noncompliance enhances the likelihood of compliance, and sanction policies are recognized as usual and necessary component of an adequate security program. ³⁵ Furthermore, the covered entity is required to identify the security official who is responsible for the development and implementation of the policies and procedures required by the security regulations for the entity. ³⁶
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)	Addressable- The covered entity should determine whether it should implement policies and procedures to authorize and/or supervise member of its workforce who have access to EPHI or in locations where it might be accessed. ³⁷ Recognizing that maintenance personnel cannot always be supervised by a knowledgeable person, the preamble to the final regulations indicated that workforce members must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see §164.308(a)(3)(ii)(A)). ³⁸
		Workforce Clearance Procedure	(A)	Addressable - The covered entity must determine if it should have procedures to determine that the access of a workforce member to EPHI is appropriate. ³⁹ An effective personnel screening process

³⁵ 68 F.R. 8347 (2003).

³⁶ 45 C.F.R. §164.308(a)(2) (2003).

³⁷ 45 C.F.R. §164.308(a)(3)(ii)(A) (2003).

³⁸ 68 F.R. 8348 (2003).

³⁹ 45 C.F.R. §164.308(a)(3)(ii)(B) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
				may be applied in a way to allow a range of implementation, from minimal to more stringent procedures based on the risk analysis performed by the covered entity. ⁴⁰
		Termination Procedures Key and password turn in and locking employees out of system after termination of employment. ⁴¹	(A)	Addressable -The covered entity must assess whether it should have procedures to terminate an individual's access to EPHI when the individual's employment is terminated or if the individual does not pass the workforce clearance procedure or alternative method of addressing the workforce clearance implementation specification. ⁴²
Information Access Management This standard requires the covered entity to implement policies and procedures for authorizing access to EPHI that are consistent with the requirements of the Privacy Regulations. ⁴³	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)	Required -This only applies if a health care clearinghouse is part of a larger organization to require that the health care clearinghouse function implement policies and procedures to protect the EPHI of the health care clearinghouse from the unauthorized access by the rest of the organization. ⁴⁴

⁴⁰ 68 F.R. 8348 (2003).

⁴¹ 68 F.R. 8348-8349 (2003).

⁴² 45 C.F.R. §164.308(a)(3)(ii)(C) (2003).

⁴³ 45 C.F.R. §164.308(a)(4)(i) (2003).

⁴⁴ 45 C.F.R. §164.308(a)(4)(ii)(A) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
		Access Authorization	(A)	Addressable -The covered entity must assess whether it should implement policies and procedures to grant access the EPHI, such as through a specific workstation, program, transaction or other mechanism. ⁴⁵
		Access Establishment and Modification	(A)	Addressable - The covered entity must assess whether it should implement policies and procedures that based upon the entity's access authorization policies (above) establish, document , review, and modify a user's right to access to a workstation, transaction, program or process. ⁴⁶
Security Awareness and Training- This standard requires the covered entity to implement a security awareness and training program for all members of its workforce, including management. ⁴⁷	164.308(a)(5)	Security Reminders	(A)	Addressable -The covered entity should address whether or how it should implement periodic security updates. ⁴⁸
		Protection from Malicious Software	(A)	Addressable - The covered entity should address how it will implement procedures that will guard against and detect and report malicious software (e.g., viruses or a virus reminder). ⁴⁹
		Log-in Monitoring	(A)	Addressable -The covered entity should address how it will implement procedures that will monitor log-in attempts and report any discrepancies. ⁵⁰

⁴⁵ 45 C.F.R. §164.308(a)(4)(ii)(B) (2003).

⁴⁶ 45 C.F.R. §164.308(a)(4)(ii)(C) (2003).

⁴⁷ 45 C.F.R. §164.308(a)(5)(i) (2003).

⁴⁸ 45 C.F.R. §164.308(a)(5)(ii)(A) (2003).

⁴⁹ 45 C.F.R. §164.308(a)(5)(ii)(B) (2003).

⁵⁰ 45 C.F.R. §164.308(a)(5)(ii)(C) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
		Password Management	(A)	Addressable -The covered entity must determine what procedures it must establish for password creation, change and safeguarding. ⁵¹ For example, establishing a policy prohibiting posting passwords on post-it notes on monitors.
Security Incident Procedures	164.308(a)(6)	Response and Reporting A security incident includes the misuse of data. ⁵²	(R)	Required -The covered entity must identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. ⁵³
Contingency Plan The contingency plan involves the establishment and implementation of policies and procedures for responding to an emergency or other occurrence, such as a fire, system failure or natural disaster, that damages systems containing EPHI. ⁵⁴ A contingency plan is the only way to protect the availability, integrity and security of data during unexpected negative events. ⁵⁵	164.308(a)(7)	Data Backup Plan	(R)	Required -The covered entity must establish and implement procedures to create and maintain retrievable exact copies of EPHI. ⁵⁶

⁵¹ 45 C.F.R. §164.308(a)(5)(ii)(D) (2003).

⁵² 68 F.R. 8351 (2003).

⁵³ 45 C.F.R. §164.308(a)(6)(ii) (2003).

⁵⁴ 45 C.F.R. §164.308(a)(7) (2003).

⁵⁵ 68 F.R. 8351 (2003).

⁵⁶ 45 C.F.R. §164.308(a)(7)(ii)(A) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
		Disaster Recovery Plan	(R)	Required -The covered entity must establish and implement procedures to restore any loss of data. ⁵⁷
		Emergency Mode Operation Plan An emergency operations plan only involves those critical business processes that must occur to protect the security of EPHI during and immediately after a crisis situation. ⁵⁸	(R)	Required -The covered entity must establish and implement procedures to enable continuation of critical business processes for the protection of security of EPHI. ⁵⁹
		Testing and Revision Procedure	(A)	Addressable -The covered entity must assess how it will meet the standard and whether it needs to establish and implement procedures to periodically test and revise its contingency plan. ⁶⁰
		Applications and Data Criticality Analysis	(A)	Addressable - The covered entity must assess the relative criticality of specific applications and data in support of other contingency plan components. ⁶¹

⁵⁷ 45 C.F.R. §164.308(a)(7)(ii)(A) (2003).

⁵⁸ 68 F.R. 8351 (2003).

⁵⁹ 45 C.F.R. §164.308(a)(7)(ii)(C) (2003).

⁶⁰ 45 C.F.R. §164.308(a)(7)(ii)(D) (2003).

⁶¹ 45 C.F.R. §164.308(a)(7)(ii)(E) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification	
Evaluation	164.308(a)(8)		(R)	Required -Covered entities are to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the final security regulations, in response to environmental or operational changes that affect the security of EPHI , that establish the extent to which the covered entity’s security policies and procedures meet the requirements of the final security regulations. ⁶² Covered entities are to periodically assess their security safeguards to demonstrate and document their compliance with the organization’s security policies and the regulations.If the covered entity has changes to its security environment, it must assess the need for a new evaluation based upon the changes that were made. A covered entity may comply by using its own workforce or an external accreditation agency that acts as a business associate. ⁶³ Reassessment of how policies are working needs to be periodically done.
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)	Required -A covered entity may permit a business associate to create, receive, maintain or transmit EPHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances in a written agreement that the business associate will safeguard the information in a written agreement that complies with 45 C.F.R. §164.314(a) (2003). ⁶⁴ This means that the business associate agreement must be modified to require the business associate to (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI it creates, maintains, receives or transmits on behalf of the covered entity; (2) ensures that any agent, including a subcontractor, to whom it provides such EPHI agrees to implement reasonable and appropriate safeguards to

⁶² 45 C.F.R. §164.308(a)(8) (2003).

⁶³ 68 F.R. 8351 (2003).

⁶⁴ 45 C.F.R. §164.308(b) (2003).

HIPAA FINAL SECURITY REGULATIONS § 164.308 - ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification
			<p>protect it; (3) report to the covered entity any security incident of which it becomes aware; and (4) authorizes termination of the agreement if the covered entity determines that the business associate has violated a material term of the contract.⁶⁵ Different requirements apply when a covered entity and its business associate are both governmental entities, see 45 C.F.R. §164.314(a)(2)(ii) (2003). If a covered entity is a business associate of another covered entity and the covered entity violates the satisfactory assurances it provided to the other covered entity, the violating business associate/covered entity will be in violation of the implementation specifications under the security regulations.⁶⁶</p>

⁶⁵ 45 C.F.R. § 164.314(a) (2003).

⁶⁶ 45 C.F.R. § 164.308(b)(3) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.310– PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable		Description of Implementation Specification
<p>Facility Access Controls-The covered entity must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed to ensure that only properly authorized access is allowed.⁶⁷</p>	<p>164.310(a)(1)</p>	<p>Contingency Operations- This is intended to include disaster recovery and emergency mode operations.⁶⁸</p>	<p>(A)</p>	<p>Addressable-The covered entity must address implementation of policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are located, while ensuring that only properly authorized access is allowed.⁶⁹</p>
		<p>Facility Security Plant Facility security is the responsibility of the covered entity even if it shares space within a building. The facility security measures taken by a third party must be considered and documented in the covered entity’s security plan, when appropriate.⁷⁰</p>	<p>(A)</p>	<p>Addressable-The covered entity must address implementation of policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.⁷¹</p>

⁶⁷ 45 C.F.R. §164.310(a) (2003).

⁶⁸ 68 F.R. 8353 (2003).

⁶⁹ 45 C.F.R. §164.310(a)(2)(i) (2003).

⁷⁰ 68 F.R. 8353 (2003).

⁷¹ 45 C.F.R. §164.310(a)(2)(ii) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.310– PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification
		Access Control and Validation Procedures	(A) Addressable -The covered entity must address implementation of policies and procedures to control and validate a person’s access to facilities based upon their role or function, including visitor control, and control of access to software programs for testing and revision. ⁷²
		Maintenance Records	(A) Addressable -The covered entity must address implementation of policies and procedures to document repairs and modifications to the physical components of a facility which are related to security, such as hardware, walls, doors, and locks. ⁷³
Workstation Use	164.310(b)		(R) Required - This involves the implementation of 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 EPHI. ⁷⁴ For example, privacy screens added to computer monitors so they are not viewable at an angle.

⁷² 45 C.F.R. §164.310(a)(2)(iii) (2003).

⁷³ 45 C.F.R. §164.310(a)(2)(iv) (2003).

⁷⁴ 45 C.F.R. §164.310(b) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.310– PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specification
Workstation Security	164.310(c)		(R) Required --The covered entity must implement physical safeguards for all workstations that access EPHI to restrict access to authorized users. ⁷⁵ This includes laptops and home office computers used to access EPHI because the definition is an electronic computing device or any other device that performs similar functions and including the electronic media stored in its immediate environment. ⁷⁶
Device and Media Controls – The covered entity must implement policies and procedures that govern the receipt and removal of hardware and electronic media containing EPHI into and out of the facility and the movement of those items within the facility. ⁷⁷ This is intended to cover both the physical premises and the interior and exterior of the building(s). ⁷⁸	164.310(d)(1)		(R) Required --The covered entity must implement policies and procedures to address the final disposal of EPHI and/or the hardware or electronic media on which it is stored. ⁷⁹
		Media Re-use	(R) Required --The covered entity must implement policies and procedures for removal of all EPHI from electronic media before it is made available for re-use. ⁸⁰

⁷⁵ 45 C.F.R. §164.310(c) (2003).

⁷⁶ 68 F.R. 8354 (2003) and 45 C.F.R. §164.304 (2003).

⁷⁷ 45 C.F.R. §164.310(d)(1) (2003).

⁷⁸ 68 F.R. 8354 (2003).

⁷⁹ 45 C.F.R. §164.310(d)(2)(i) (2003).

⁸⁰ 45 C.F.R. §164.310(d)(2)(ii) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.310– PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable		Description of Implementation Specification
		Accountability	(A)	Addressable --The covered entity must address maintaining a record of the movements of hardware and electronic media and any person responsible therefore. ⁸¹
		Data Backup and Storage	(A)	Addressable --The covered entity must address creating a retrievable, exact copy of EPHI, when needed, before movement of equipment. ⁸²

⁸¹ 45 C.F.R. §164.310(d)(2)(iii) (2003).

⁸² 45 C.F.R. §164.310(d)(2)(iv) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.312 - TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable		Description of Implementation Specifications
Access Controls- The covered entity must implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights under the Information Access Management Standard under the Administrative Safeguards. ⁸³	164.312(a)(1)	Unique User Identification	(R)	Required- The covered entity must assign a unique name and/or number for identifying and tracking user identity. ⁸⁴
		Emergency Access Procedure	(R)	Required- The covered entity must establish, and implement, as needed, procedures for obtaining necessary EPHI. ⁸⁵
		Automatic Logoff	(A)	Addressable- The covered entity must address whether or not to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. ⁸⁶

⁸³ 45 C.F.R. §164.312(a) (2003).

⁸⁴ 45 C.F.R. §164.312(a)(2) (2003).

⁸⁵ 45 C.F.R. §164.312(a)(2) (2003).

⁸⁶ 45 C.F.R. §164.312(a)(2) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.312 - TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable	Description of Implementation Specifications
Audit Controls	164.312(b)	The audit control is a mandatory requirement because it provides a means to assess activities regarding the electronic protected health information that is in the entity's care. ⁸⁷	(R) Required- The covered entity must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. ⁸⁸ For example, document history is tracked in some software to identify who has accessed the document.
Integrity- The covered entity must implement policies and procedures to protect EPHI from improper alteration or destruction. ⁸⁹	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A) Addressable- The covered entity must address whether or not to implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. ⁹⁰
Person or Entity Authentication	164.312(d)		(R) Required- The covered entity must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed. ⁹¹

⁸⁷ 68 F.R. 8355 (2003).

⁸⁸ 45 C.F.R. §164.312(b) (2003).

⁸⁹ 45 C.F.R. §164.312(c)(1) (2003).

⁹⁰ 45 C.F.R. §164.312(c)(2) (2003).

⁹¹ 45 C.F.R. §164.312(d) (2003).

HIPAA FINAL SECURITY REGULATIONS §164.312 - TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable		Description of Implementation Specifications
Transmission Security -The covered entity must implement security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. ⁹²	164.312(e)(1)	Integrity Controls	(A)	Addressable -The covered entity must address whether or not to implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until such EPHI is disposed of. ⁹³
	164.312(d)(1)	Encryption	(A)	Addressable -The covered entity must address whether or not to implement a mechanism to encrypt EPHI whenever the covered entity deems it to be appropriate. ⁹⁴

D-1120848.10

⁹² 45 C.F.R. §164.312(e)(1) (2003).

⁹³ 45 C.F.R. §164.312(e)(2) (2003).

⁹⁴ 45 C.F.R. §164.312(d)(2) (2003).