2.) **The Security Rule** *(Part 164, Subpart C)*

- § 164.302 – Applicability
- § 164.304 – Definitions
- § 164.306 – Security standards: General rules
- § 164.308 – Administrative safeguards
- § 164.310 – Physical safeguards
- § 164.312 – Technical safeguards
- § 164.314 – Organizational requirements
- § 164.316 – Policies and procedures and documentation requirements

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.302 – Applicability	Covered entities must comply with the requirements of the Security Rule with respect to electronic protected health information.[1]	The Proposed Rule applied this section to business associates.[2]	Adopts as proposed.[3]

[1] 45 C.F.R. § 164.302 (2007).
[2] 75 Fed. Reg. at 40882.
[3] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.106.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.304 – Definitions	*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.[4] *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.[5] *Access* is the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource; this definition does not apply to "access" as used in the Privacy Rule.[6]	The Proposed Rule inserted reference to business associates in the definitions of *administrative safeguards* and *physical safeguards*.[7] The Interim Final Breach Notification Rule amended the definition of *access* to note that the definition also does not apply to "access" as used within the Breach Notification Rule.[8]	Adopts as proposed.[9]
§ 164.306 – Security standards:	Generally, a covered entity must: (1) ensure the confidentiality, integrity, and	The Proposed Rule applied the general requirements for security standards to	Adopts as proposed.[20]

[4] 45 C.F.R. § 164.304, at "Administrative safeguards" (2007).
[5] 45 C.F.R. § 164.304, at "Physical safeguards" (2007).
[6] 45 C.F.R. § 164.304, at "Access" (2007).
[7] 75 Fed. Reg. at 40882.
[8] 74 Fed. Reg. at 42756.
[9] 78 Fed. Reg. at 5693; 45 C.F.R. § 164.304.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
General rules	availability of all of the electronic protected health information it creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures that are not permitted or required under the Privacy Rule; and (4) ensure that its workforce complies with the requirements of the Security Rule.[10] Covered entities must comply with the standards provided in the Security Rule with respect to all electronic protected health information.[11] Most standards identified in the Security Rule include implementation specifications. Implementation specifications are either "required" or "addressable."[12] Covered entities must implement all "required" implementation specifications as written.[13] If an implementation specification is "addressable," the covered entity must assess whether, in	business associates in the same manner as they apply to covered entities.[19]	

[20] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.306.
[10] 45 C.F.R. § 164.306(a) (2007).
[11] 45 C.F.R. § 164.306(c) (2007) (referencing the requirements of this section and at §§ 164.308, 164.310, 164.312, 164.314, and 164.316).
[12] 45 C.F.R. § 164.306(d)(1) (2007).
[13] 45 C.F.R. § 164.306(d)(2) (2007).
[19] 75 Fed. Reg. at 40882.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	the covered entity's environment, the specification would reasonably and appropriately safeguard the covered entity's electronic protected health information.[14] If it would, the covered entity must implement the specification. If it would not, the covered entity must document why, and, if reasonable and appropriate, adopt an equivalent alternative measure.[15] A covered entity may use any security measures to satisfy the Security Rule's standards and implementation specifications.[16] When deciding what measures to use, the covered entity must take four specific factors into account.[17] The covered entity must review the security measures it uses and modify them as needed.[18]		
§ 164.308 – Administrative safeguards	There are eight administrative safeguard standards covered entities must satisfy. The first standard requires covered entities to have a security management process that includes policies and	The Proposed Rule applied this section to business associates in the same manner as it applies to covered entities.[41] The Proposed Rule makes a technical	Adopts as proposed.[44]

[14] 45 C.F.R. § 164.306(d)(3)(i) (2007).
[15] 45 C.F.R. § 164.306(d)(3)(ii) (2007).
[16] 45 C.F.R. § 164.306(b)(1) (2007).
[17] 45 C.F.R. § 164.306(b)(2) (2007).
[18] 45 C.F.R. § 164.306(e) (2007) (Note that security measures must provide reasonable and appropriate protection of electronic protected health information as described in § 164.316).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	procedures to prevent, detect, contain and correct security violations.[21] There are four required implementation specifications: (i) conduct a risk analysis; (ii) implement risk management measures; (iii) enforce a sanction policy; and (iv) implement procedures to review information system activity records.[22] The second standard requires covered entities to assign responsibility for the development and implementation of the policies and procedures required by the Security Rule.[23] The third standard requires covered entities to implement workforce security policies and procedures to ensure appropriate access to electronic protected health information.[24] There are three addressable implementation specifications: (i) implement procedures for authorization and/or supervision; (ii) implement workforce clearance procedures; and (iii) implement procedures for terminating access.[25]	change to the third standard's specification requiring implementation of access termination procedures, such that the procedures for terminating access apply when the workforce member's employment **or other arrangement** ends, reflecting that some workforce members are not employees (i.e., may be volunteers). The Proposed Rule made several modifications to the standard governing business associate arrangements. It removed the provision excluding application of this standard to situations that do not give rise to a business associate relationship, as such exceptions are now included within the definition of *business associate*.[42] It added provisions to clarify that covered entities are not required to obtain satisfactory assurances from a subcontractor, but that business associates are required to do so.[43] It removed the provision holding a business associate that is also a covered entity responsible for its violation of	

[41] 75 Fed. Reg. at 40882.
[44] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.308.
[21] 45 C.F.R. § 164.308(a)(1)(i) (2007).
[22] 45 C.F.R. § 164.308(a)(1)(ii) (2007).
[23] 45 C.F.R. § 164.308(a)(2) (2007).
[24] 45 C.F.R. § 164.308(a)(3)(i) (2007).
[25] 45 C.F.R. § 164.308(a)(3)(ii) (2007).
[42] 75 Fed. Reg. at 40882.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	The fourth standard requires covered entities to implement policies and procedures for information access management that are consistent with the applicable requirements of the Privacy Rule.[26] There is one required implementation specification: isolate health care clearinghouse functions from unauthorized access,[27] and two addressable implementation specifications: (i) implement policies and procedures for access authorization,[28] and (ii) implement policies and procedures to establish and modify access.[29] The fifth standard requires covered entities to implement a security awareness and training program for all members of its workforce.[30] There are four addressable implementation specifications: (i) implement periodic security updates; (ii) implement procedures to protect against malicious software; (iii) implement procedures to	this standard and § 164.314(a) as a covered entity. There is no longer a need to apply specific provisions to business associates, as the provisions of the Security Rule now apply to business associates in the same manner as they apply to covered entities.	

[43] 75 Fed. Reg. at 40883.
[26] 45 C.F.R. § 164.308(a)(4)(i) (2007).
[27] 45 C.F.R. § 164.308(a)(4)(ii)(A) (2007).
[28] 45 C.F.R. § 164.308(a)(4)(ii)(B) (2007).
[29] 45 C.F.R. § 164.308(a)(4)(ii)(C) (2007).
[30] 45 C.F.R. § 164.308(a)(5)(i) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	monitor log-ins; and (iv) implement procedures for password management.[31] The sixth standard requires covered entities to implement policies and procedures to address security incidents.[32] There is one required implementation specification: implement security incident response and reporting.[33] The seventh standard requires covered entities to establish and implement as needed a contingency plan.[34] There are three required implementation specifications: (i) establish and implement a data backup plan; (ii) establish (and implement as needed) a disaster recovery plan; and (iii) establish (and implement as needed) an emergency mode operation plan, and two addressable implementation specifications: (i) implement procedures for testing and revision of contingency plans; and (ii) assess the criticality of applications and data.[35] The eighth standard requires covered		

[31] 45 C.F.R. § 164.308(a)(5)(ii) (2007).
[32] 45 C.F.R. § 164.308(a)(6)(i) (2007).
[33] 45 C.F.R. § 164.308(a)(6)(ii) (2007).
[34] 45 C.F.R. § 164.308(a)(7)(i) (2007).
[35] 45 C.F.R. §164.308(a)(7)(ii) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	entities to perform a periodic technical and nontechnical evaluation to establish the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.[36] An additional standard, which is applicable to a covered entity that chooses to permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf, requires such covered entity to obtain satisfactory assurances that the business associate will appropriately safeguard [protected health] information, through a business associate contract or other arrangement.[37] There is one required implementation specification: document the required assurances in a written contract or through another arrangement that meets the requirements of § 164.314(a).[38] If a business associate is itself a covered entity, it is responsible for complying with these provisions (and with § 164.314(a)) to the same extent as a covered entity.[39] This standard is not applicable to covered entities in certain situations that do not		

[36] 45 C.F.R. § 164.308(a)(8) (2007).
[37] 45 C.F.R. § 164.308(b)(1) (2007).
[38] 45 C.F.R. § 164.308(b)(4) (2007) (referencing applicable requirements in § 164.314(a)).
[39] 45 C.F.R. §164.308(b)(3) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	give rise to a business associate relationship.[40]		
§ 164.310 – Physical safeguards	There are four physical safeguard standards covered entities must satisfy. The first standard requires covered entities to implement facility access controls.[45] There are four addressable implementation specifications: (i) establish and implement contingency operations procedures; (ii) implement a facility security plan; (iii) implement access control and validation procedures; and (iv) implement policies and procedures to document maintenance of the facility's physical components that are related to security.[46] The second standard requires covered entities to implement workstation use policies and procedures.[47] The third standard requires covered entities to implement physical safeguards for all workstations that access electronic protected health information.[48]	The Proposed Rule applied this section to business associates in the same manner that it applies to covered entities.[51]	Adopts as proposed.[52]

[40] 45 C.F.R. § 164.308(b)(2) (2007).
[45] 45 C.F.R. § 164.310(a)(1) (2007).
[46] 45 C.F.R. § 164.310(a)(2) (2007).
[47] 45 C.F.R. §164.310(b) (2007).
[48] 45 C.F.R. § 164.310(c) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	The fourth standard requires covered entities to implement device and media control policies and procedures.[49] There are two required implementation specifications: (i) implement disposal policies and procedures and (ii) implement media re-use procedures, and two addressable implementation specifications: (i) maintain records accounting for movement of media and the persons responsible, and (ii) backup/store data before moving equipment.[50]		
§ 164.312 – Technical safeguards	There are five technical safeguard standards covered entities must satisfy. The first standard requires covered entities to implement technical policies and procedures for electronic information systems to control access.[53] There are two required implementation specifications: (i) assign unique user identifications; and (ii) establish (and implement as needed) emergency access procedures, and two addressable implementation specifications: (i) implement automatic logoff procedures;	The Proposed Rule applied this section to business associates in the same manner as it applies to covered entities.[61]	Adopts as proposed.[62]

[51] 75 Fed. Reg. at 40882.
[52] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.310.
[49] 45 C.F.R. § 164.310(d)(1) (2007).
[50] 45 C.F.R. § 164.310(d)(2) (2007).
[53] 45 C.F.R. § 164.312(a)(1) (2007) (referencing access rights specified in § 164.308(a)(4)).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	and (ii) implement a mechanism to encrypt and decrypt electronic protected health information.[54] The second standard requires covered entities to implement audit controls.[55] The third standard requires covered entities to implement policies and procedures to protect the integrity of electronic protected health information.[56] There is one addressable implementation specification: implement mechanisms to authenticate electronic protected health information.[57] The fourth standard requires covered entities to implement procedures to authenticate the identity of a person or entity seeking access to electronic protected health information.[58] The fifth standard requires covered entities to implement technical transmission security measures.[59] There		

[61] 75 Fed. Reg. at 40882.
[62] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.312.
[54] 45 C.F.R. § 164.312(a)(2) (2007).
[55] 45 C.F.R. § 164.312(b) (2007).
[56] 45 C.F.R. § 164.312(c)(1) (2007).
[57] 45 C.F.R. § 164.312(c)(2) (2007).
[58] 45 C.F.R. § 164.312(d) (2007).
[59] 45 C.F.R. § 164.312(e)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	are two addressable implementation specifications: (i) implement integrity controls; and (ii) implement an encryption mechanism.[60]		
§ 164.314 – Organizational requirements	There are two organizational requirement standards that a covered entity must satisfy, as applicable. If a covered entity chooses to permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf, the first standard requires that the contract or other arrangement between that covered entity and its business associate[63] satisfy the applicable implementation specification.[64] If a covered entity knows of a material breach or violation of the business associate's obligation under the contract or other arrangement, it must take specific steps to deal with the violation; failure to take these steps constitutes a violation of this standard, and of § 164.502(e).[65]	The Proposed Rule added a paragraph applying the requirements of the first standard to agreements between business associates and subcontractors in the same manner as it applies to agreements between covered entities and business associates. [69] The Proposed Rule modified element (B) of the business associate contract implementation specification, so that a business associate must agree to ensure that its subcontractors enter into a contract or other arrangement that complies with this section.[70] The Proposed Rule also modified contract element (C), so that a business associate must specifically agree to report breaches of unsecured protected health information as required.	Adopts as proposed.[71]

[60] 45 C.F.R. § 164.312(e)(2) (2007).

[63] Note that the standard at paragraph (b)(1) of the administrative safeguard provisions (§ 164.308) (which is applicable only to covered entities that choose to permit business associates to create, receive, maintain, or transmit electronic protected health information on their behalf) requires the covered entity to obtain satisfactory assurances that the business associate will appropriately safeguard the information; the single implementation specification for this administrative safeguard standard requires the covered entity to document these satisfactory assurances through a written contract or other arrangement with the business associate that meets the applicable requirements of this section (§ 164.314).

[64] 45 C.F.R. § 164.314(a)(1)(i) (2007).

[65] 45 C.F.R. § 164.314(a)(1)(ii) (2007).

[69] 75 Fed. Reg. at 40883.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	The implementation specification for business associate contracts sets forth four required contract elements: (A) implement required safeguards that protect the electronic protected health information; (B) ensure that any agent (including a subcontractor) agrees to implement safeguards to protect the information; (C) report any security incident of which it becomes aware; and (D) authorize the covered entity to terminate the contract if the covered entity determines that the business associate has violated a material term.[66] The implementation specification for "other arrangements" set forth requirements applicable to three specific types of arrangements.[67] The second standard sets forth requirements applicable to a group health plan.[68]	The Proposed Rule removed both the provision detailing the steps a covered entity must take to deal with a breach or violation of the contract and contract element (D). The Proposed Rule modified the implementation specification for "other arrangements" by removing the specific requirements applicable to three types of "other arrangements," and adding a provision stating that a covered entity satisfies the first standard if it its arrangement meets the requirements of § 164.504(e)(3).	
§ 164.316 – Policies and procedures and documentation	There is one policy and procedure standard, which requires covered entities to implement policies and	The Proposed Rule applied this section to business associates in the same manner as it applies to covered	Adopts as proposed.[76]

[70] 75 Fed. Reg. at 40883.
[71] 78 Fed. Reg. at 5591; 45 C.F.R. § 164.314.
[66] 45 C.F.R. § 164.314(a)(2)(i) (2007).
[67] 45 C.F.R. § 164.314(a)(2)(ii) (2007).
[68] 45 C.F.R. § 164.314(b) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
requirements	procedures to comply with the Security Rule requirements.[72] A covered entity may change its policies and procedures at any time, but must document and implement the changes in accordance with the Security Rule. There is one documentation standard, which requires covered entities to maintain these policies and procedures in written form and, as required, a written record of any action, activity or assessment.[73] This standard has three required implementation specifications: (i) retain required documentation for a specific time period; (ii) make documentation available as required; and (iii) update documentation as needed.[74]	entities.[75]	

[76] 78 Fed. Reg. at 5695; 45 C.F.R. § 164.316.
[72] 45 C.F.R. § 164.316(a) (2007).
[73] 45 C.F.R. § 164.316(b)(1) (2007) (Note that "written form" may be electronic).
[74] 45 C.F.R. § 164.316(b)(2) (2007).
[75] 75 Fed. Reg. at 40882.