

6.) General Provisions Applicable to Part 164 - the Security, Breach Notification, and Privacy Rules (Part 164, Subpart A)

- § 164.102 – Statutory basis
- § 164.103 – Definitions (law enforcement official)
- § 164.104 – Applicability
- § 164.105 – Organizational requirements
- § 164.106 – Relationship to other parts

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.102 – Statutory basis	The requirements in Part 164 are adopted in accordance with the Secretary’s authority under Title 11, Part C of the Social Security Act and HIPAA § 264. ¹	The Proposed Rule added HITECH §§ 13400 – 13424 as a basis for the authority to prescribe the requirements in Part 164. ²	Adopts as proposed. ³

¹ 45 C.F.R. § 164.102 (2007).

² 75 Fed. Reg. at 40881 (Note that the Breach Notification Interim Final Rule added a reference to HITECH § 13402, which was adopted as of 2009 in the CFR).

³ 78 Fed. Reg. at 5587; 45 C.F.R. § 164.102.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
<p>§ 164.103 – Definitions, <i>law enforcement official</i></p>	<p>The HIPAA provisions do not define <i>law enforcement official</i> at § 164.103.</p> <p>At § 164.501, <i>law enforcement official</i> is “an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.”⁴</p>	<p>The Interim Final Breach Notification Rule moved the definition of <i>law enforcement official</i> from § 164.501 to § 164.103, so that it applies to both the Breach Notification and Privacy Rules.⁵</p>	<p>Retains without modification.⁶</p>
<p>§ 164.104 – Applicability</p>	<p>The provisions of Part 164 apply to <i>covered entities</i>, which include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the HIPAA rules.⁷</p> <p>When a health care clearinghouse creates or receives protected health</p>	<p>The Proposed Rule applied the provisions of Part 164 to business associates where specified.⁹</p> <p>The Proposed Rule removed the language requiring a health care clearinghouse to comply with § 164.105.</p>	<p>Adopts as proposed.¹⁰</p>

⁴ 45 C.F.R. § 164.501, at “Law enforcement official” (2007).

⁵ 74 Fed. Reg. at 42755.

⁶ 78 Fed. Reg. at 5566; 45 C.F.R. § 164.103, at “Law enforcement official.”

⁷ 45 C.F.R. § 164.104(a) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	information as it must comply with the organizational requirements for covered entities in §164.105. ⁸		
§ 164.105 – Organizational requirements	Only the health care components of a hybrid covered entity are subject to the Privacy and Security Rules, with specific exceptions. ¹¹ A hybrid covered entity must designate any components that perform covered functions as “health care components,” including any component that would be considered a “covered entity” if it were a legally separate entity from the hybrid covered entity. ¹² A hybrid covered entity has discretion to include other components to the extent that they perform covered functions or to the extent that they perform “business associate-like activities” (i.e., activities that would make the component a business associate of a component that performs covered functions, if both components were separate legal	<p>The Proposed Rule replaced all references to the Security and/or Privacy Rules with a reference to “part 164,” to make clear that the Security Rule (at subpart C), the Privacy Rule (at subpart E), and the new Breach Notification Rule (at subpart D) all apply with respect to the provisions of this section.¹⁹</p> <p>The Proposed Rule removed the provision that specifically required a covered entity to ensure that business associate-like components included in its health care component comply with the Privacy and Security Rules, as this oversight obligation is already established elsewhere in the Rule.²⁰</p>	<p>Adopts as proposed.²¹</p> <p>The Final Rule modifies the provision requiring a hybrid covered entity to designate which components are part of its health care component(s), so that a hybrid covered entity is required to include any component that would meet the definition of “business associate” if it were a separate legal entity from the hybrid covered entity.²² The Final Rule retains a hybrid covered entity’s discretion to include in its health care component other components to the extent they perform covered functions.</p>

⁹ 75 Fed. Reg. at 40881.

¹⁰ 78 Fed. Reg. at 5587 -88; 45 C.F.R. § 164.104(b).

⁸ 45 C.F.R. § 164.104(b) (2007).

¹¹ 45 C.F.R. § 164.105(a)(1) (2007) (Note that the requirements of §§164.105, 164.314 and 164.504 apply to the entire covered entity).

¹² 45 C.F.R. § 164.105(a)(2)(iii)(C) (2007).

¹⁹ 75 Fed. Reg. at 40881.

²⁰ 75 Fed. Reg. at 40882.

²¹ 78 Fed. Reg. at 5588; 45 C.F.R. § 164.105.

²² 78 Fed. Reg. at 5588; 45 C.F.R. § 164.105(a)(2)(iii)(D).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	<p>entities).</p> <p>The hybrid covered entity retains certain oversight, compliance and enforcement obligations. It must ensure that its health care component(s) comply with the applicable requirements of this section and the Privacy and Security Rules.¹³ It must also ensure that any component that performs business associate-like activities that is included in its health care component complies with the Privacy and Security Rules.¹⁴ The hybrid covered entity is ultimately responsible for compliance with the Privacy Rule for purposes of the [compliance and enforcement provisions] of the Enforcement Rule,¹⁵ and it must also implement policies and procedures to ensure compliance with this section and the Privacy and Security Rules.¹⁶</p> <p>Legally affiliated covered entities may designate themselves as a single</p>	<p>The Proposed Rule added a new paragraph making the hybrid covered entity itself responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements in this section.</p> <p>The Proposed Rule combined the safeguarding provisions applicable to affiliated covered entities into one provision.</p>	

¹³ 45 C.F.R. § 164.105(a)(2)(ii) (2007).

¹⁴ 45 C.F.R. § 164.105(a)(2)(ii)(C), (D) (2007).

¹⁵ 45 C.F.R. § 164.105(a)(2)(iii)(A) (2007).

¹⁶ 45 C.F.R. § 164.105(a)(2)(iii)(B) (2007) (referencing policies and procedures in §§ 164.316(a) and 164.530(i)).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	covered entity for purposes of the Privacy and Security Rules, if all of the designated covered entities are under common ownership or control. ¹⁷ For safeguarding purposes, an affiliated covered entity must ensure that it: (A) complies with the applicable requirements of the Security Rule; (B) complies with applicable requirements of the Privacy Rule; and (C) if it combines the functions of a health plan, health care provider, or health care clearinghouse, complies with §§ 164.308(a)(4)(ii)(A) and 164.504(g), as applicable. ¹⁸		

¹⁷ 45 C.F.R. § 164.105(b)(1) (2007) (referencing documentation requirements at § 164.105(c)).

¹⁸ 45 C.F.R. § 164.105(b)(1)(ii) (2007)