4.) <u>The Enforcement Rule</u> (*Part 160, Subparts C, D, and E*)

- § 160.300 – Applicability
- § 160.304 – Principles for achieving compliance
- § 160.306 – Complaints to the Secretary
- § 160.308 – Compliance reviews
- § 160.310 – Responsibilities of covered entities
- § 160.312 – Secretarial action regarding complaints and compliance reviews
- § 160.316 – Refraining from intimidation or retaliation
- § 160.401 – Definitions
- § 160.402 – Basis for a civil money penalty
- § 160.404 – Amount of a civil money penalty
- § 160.406 – Violations of an identical requirement or prohibition
- § 160.408 – Factors considered in determining the amount of a civil money penalty
- § 160.410 – Affirmative defenses § 160.418 – Penalty not exclusive
- § 160.420 – Notice of proposed determination
- § 160.534 – The hearing

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 160.300 – Applicability	The provisions of the Enforcement Rule governing compliance and investigations apply to covered entities.[1]	The Proposed Rule added that these provisions apply to business associates.[2]	Adopts as proposed.[3]
§ 160.304 – Principles for achieving compliance	To the extent practicable, the Secretary will seek the cooperation of covered entities in obtaining compliance with the applicable HIPAA provisions.[4] The Secretary may provide technical assistance to covered entities to help them comply voluntarily.[5]	The Proposed Rule added that the Secretary will seek cooperation consistent with the [compliance and investigations] provisions, and applied this section to business associates such that the Secretary will also seek their cooperation as applicable and may provide them with technical assistance.[6]	Adopts as proposed.[7]
§ 160.306 – Complaints to the Secretary	A person who believes a covered entity is not complying with HIPAA may file a complaint with the Secretary,[8] who may choose to investigate such complaints.[9]	The Proposed Rule applied this provision to business associates. The Proposed Rule required the Secretary to investigate all complaints where a "preliminary review of the facts indicates a possible violation due to willful neglect," but retained the Secretary's discretion to investigate any other complaints.[10]	Adopts as proposed.[11]
§ 160.308 – Compliance reviews	The Secretary may conduct compliance reviews to determine whether covered	The Proposed Rule applied this provision to business associates. The	Adopts as proposed.[14]

[1] 45 C.F.R. § 160.300 (2007).
[2] 75 Fed. Reg. at 40875.
[3] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.300.
[4] 45 C.F.R. § 160.304(a) (2007).
[5] 45 C.F.R. § 160.304(b) (2007).
[6] 75 Fed. Reg. at 40875-76.
[7] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.304.
[8] 45 C.F.R. § 160.306(a) (2007).
[9] 45 C.F.R. § 160.306(c) (2007).
[10] 75 Fed. Reg. at 40876.
[11] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.306.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	entities are complying with the applicable HIPAA provisions.[12]	Proposed Rule required the Secretary to conduct compliance reviews when a "preliminary review of the facts indicates a possible violation due to willful neglect," but retained the Secretary's discretion to conduct compliance reviews in any other circumstances.[13]	
§ 160.310 – Responsibilities of covered entities	Covered entities must keep records and submit compliance reports in accordance with the Secretary's requirements.[15] Covered entities must cooperate with the Secretary during an investigation or compliance review,[16] and must give the Secretary access to its facilities, books, records, accounts and other sources of information, including protected health information, as is necessary during normal business hours.[17] If there are exigent circumstances, a covered entity must permit the Secretary access at any time and without notice. If another entity has exclusive possession of any required information and fails or refuses to furnish the information, the covered entity must so certify and describe the	The Proposed Rule applied the requirements of this section to business associates, and re-titled the section "Responsibilities of covered entities and business associates."[20] The Proposed Rule also allowed the Secretary to disclose the protected health information she obtains when permitted under § 552a(b)(7) of the Privacy Act.[21]	Adopts as proposed.[22]

[14] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.308.
[12] 45 C.F.R. § 160.308 (2007).
[13] 75 Fed. Reg. at 40876.
[15] 45 C.F.R. § 160.310(a) (2007).
[16] 45 C.F.R. § 160.310(b) (2007).
[17] 45 C.F.R. § 160.310(c)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	efforts it has made to obtain the information.[18] The Secretary may only disclose the protected health information she obtains in connection with an investigation or compliance review as is necessary to ascertain or enforce compliance, or as otherwise required by law.[19]		
§ 160.312 – Secretarial action regarding complaints and compliance reviews	The Secretary must try to informally resolve matters of noncompliance.[23] If the matter is not resolved informally, the covered entity may submit evidence of any mitigating factors or affirmative defenses within 30 days of being notified by the Secretary that the matter was not informally resolved.[24] The Secretary will inform the covered entity in a notice of proposed determination if she finds that a civil monetary penalty should be imposed.[25]	The Proposed Rule applied this section to business associates and gave the Secretary discretion to informally resolve matters of noncompliance.[26]	Adopts as proposed.[27]
§ 160.316 – Refraining from	Covered entities may not take any	The Proposed Rule applied this section	Adopts as proposed.[30]

[20] 75 Fed. Reg. at 40876.
[21] 75 Fed. Reg. at 40876.
[22] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.310.
[18] 45 C.F.R. § 160.310(c)(2) (2007).
[19] 45 C.F.R. § 160.310(c)(3) (2007).
[23] 45 C.F.R. § 160.312(a)(1) (2007).
[24] 45 C.F.R. § 160.312(a)(3)(i) (2007) (referencing §§ 160.408 and 160.410, governing mitigating factors and affirmative defenses, respectively, as well as § 160.526, prescribing computation of the time limit from receipt of notice).
[25] 45 C.F.R. § 160.312(a)(3)(ii) (2007) (referencing § 160.420, governing notices of proposed determinations).
[26] 75 Fed. Reg. at 40876-77.
[27] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.312.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
intimidation or retaliation	intimidating or retaliatory action against an individual for: (a) filing a complaint; (b) participating in an investigation, compliance review, or hearing; or (c) opposing in good faith any act or practice that is unlawful under HIPAA, in a reasonable manner and without violating the Privacy Rule.[28]	to business associates.[29]	
§ 160.401 – Definitions	The HIPAA rules do not contain § 160.401. In § 160.410, *reasonable cause* is: circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the HIPAA provision that was violated.[31] *Reasonable diligence* is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.[32] *Willful neglect* is the conscious, intentional failure or reckless	The Interim Final Enforcement Rule added § 160.401 and included the terms *reasonable cause*, *reasonable diligence*, and *willful neglect*, as defined in § 160.410.[34] The Proposed Rule did not suggest changes to the Interim Rule's definitions of *reasonable diligence* and *willful neglect*, but did amend *reasonable cause* to: an act or omission in which a covered entity or business associate did not act with willful neglect but knew, or by exercising reasonable diligence would have known, that the act or omission violated a HIPAA provision.[35]	The Final Rule makes no changes to the Interim Final Rule's definitions of *reasonable cause* or *willful neglect*. The Final Rule adopts the Proposed Rule's definition of *reasonable cause*.[36]

[30] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.316.
[28] 45 C.F.R. § 160.316 (2007).
[29] 75 Fed. Reg. at 40875.
[31] 45 C.F.R. § 160.410(a), at "Reasonable cause" (2007).
[32] 45 C.F.R. § 160.410(a), at "Reasonable diligence" (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	indifference to the obligation to comply with the HIPAA provision that was violated.[33]		
§ 160.402 – Basis for a civil money penalty	The Secretary will impose a civil monetary penalty on a covered entity for violating a HIPAA provision.[37] If more than one covered entity was responsible for a violation, the Secretary will impose a civil monetary penalty on each responsible covered entity.[38] Covered entities that are members of an affiliated covered entity are jointly and severally liable for a violation of part 164 based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.[39] Covered entities are liable for violations based on the act or omission of any of its agents acting within the scope of agency, with the exception of its business associates in certain circumstances.[40]	The Proposed Rule applied the provisions imposing civil monetary penalties to business associates, except for the provision holding covered entities jointly and severally liable for violations of an affiliated covered entity.[41] The Proposed Rule modified the provision imposing liability for violations committed by agents, such that a covered entity's agents always include its business associates (when acting within the scope of agency), and expanded the provision so that business associates are liable for violations of their agents, including their workforce members and subcontractors, when acting within the scope of agency.	Adopts as proposed.[42]

[34] HIPAA Administrative Simplification: Enforcement; Interim Final Rule with Request for Comments, 74 Fed. Reg. 56123, at 56126 (October 30, 2009).
[35] 75 Fed. Reg. at 40877.
[36] 78 Fed. Reg. at 5580; 45 C.F.R. § 160.401.
[33] 45 C.F.R. § 160.410(a), at "Willful neglect" (2007).
[37] 45 C.F.R. § 160.402(a) (2007).
[38] 45 C.F.R. § 160.402(b)(1) (2007).
[39] 45 C.F.R. § 160.402(b)(2) (2007).
[40] 45 C.F.R. § 160.402(c) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 160.404 – Amount of a civil money penalty	The Secretary may not impose a civil monetary penalty that exceeds $100 per violation,[43] or that exceeds $25,000 for identical violations during a calendar year.[44]	The Interim Final Enforcement Rule modified this section so that the existing limits on the imposition of civil monetary penalties apply only to violations occurring before February 18, 2009.[45] The Interim Final Enforcement Rule expanded this section by establishing penalty tiers applicable to violations occurring after February 18, 2009. The tiers establish a penalty range per violation (e.g. $1,000-$5,000 per violation due to reasonable cause) and limit liability to $1.5 million for identical violations during a calendar year.[46] The Proposed Rule adopted and expanded the Interim Final Rule's tiered penalty structure by applying it to business associates in the same manner as it applied to covered entities.[47]	The Final Rule made no additional changes to the Interim Final Rule's modifications,[48] and accepted the penalty tier structure as modified by the Proposed Rule.[49]
§ 160.406 – Violations of an identical requirement or	The Secretary will determine how many violations of HIPAA provision occurred based on the nature of the covered entity's obligation to act or not	The Proposed Rule applied this section to business associates.[51]	Adopts as proposed.[52]

[41] 75 Fed. Reg. at 40879.
[42] 78 Fed. Reg. at 5581; 45 C.F.R. § 160.402.
[43] 45 C.F.R. § 160.404(b)(1)(i) (2007).
[44] 45 C.F.R. § 160.404(b)(1)(ii) (2007).
[45] 74 Fed. Reg. at 56126
[46] 74 Fed. Reg. at 56126
[47] 75 Fed. Reg. at 40875.
[48] 78 Fed. Reg. at 5577, 5583; 45 C.F.R. § 160.404.
[49] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.404.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
prohibition	act under the provision that is violated.[50] A separate violation occurs each day the covered entity is in continuing violation of a provision.		
§ 160.408 – Factors considered in determining the amount of a civil money penalty	The following factors may be considered by the Secretary in determining the amount of a civil monetary penalty: (a) the nature of the violation, in light of the purpose of the rule violated; (b) the circumstances of the violation, including the consequences; (c) the degree of the covered entity's culpability; (d) the covered entity's prior compliance or noncompliance with the HIPAA provisions; (e) the covered entity's financial condition; and (f) such other matters as justice may require.[53]	The Proposed Rule amended this section by requiring the Secretary to consider the listed factors, applying the section to business associates as applicable, and modifying the factors to: (a) the nature and extent of the violation; (b) the nature and extent of the harm resulting from the violation; (c) the history of prior compliance with the HIPAA provisions, including violations, by the covered entity or business associate; (d) the financial condition of the covered entity or business associate; and (e) such other matters as justice may require.[54]	Adopts as proposed.[55]
§ 160.410 – Affirmative defenses	The Secretary may not impose a civil monetary penalty on a covered entity for a violation if the covered entity establishes that one of three affirmative defenses exist: (1) the violation is an act punishable under § 1177 of the Social Security Act[56]; (2) the covered entity lacked knowledge of the	The Interim Final Enforcement Rule amended this section for violations occurring on or after February 18, 2009, such that the second affirmative defense is unavailable, and the third affirmative defense is modified so that the covered entity need only establish that the violation is not due to willful	The Final Rule adopts the Proposed Rule's modifications.[60]

[51] 75 Fed. Reg. at 40875.
[52] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.406.
[50] 45 C.F.R. § 160.406 (2007).
[53] 45 C.F.R. § 164.408 (2007).
[54] 75 Fed. Reg. at 40880-81.
[55] 78 Fed. Reg. at 5577, 5585; 45 C.F.R. § 160.408.
[56] Social Security Act § 1177, 42 U.S.C. § 1320d-6.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	violation and would not have known that the violation occurred by exercising reasonable diligence; or (3) the violation is due to reasonable cause and not willful neglect and is corrected either within 30 days after the covered entity knew or would have known by exercising reasonable diligence that the violation occurred, or within another time period determined by the Secretary.[57]	neglect, and is corrected within the prescribed time period.[58] The Proposed Rule made additional revisions to this section.[59] For penalties imposed prior to February 18, 2011, both covered entities and business associates may utilize the first affirmative defense. For penalties imposed after February 18, 2011, a covered entity or business associate must establish that "a penalty has been imposed under § 1177." For violations occurring prior to February 18, 2009, the Proposed Rule permitted covered entities to utilize the second affirmative defense, and modified the third defense so that a covered entity must establish that: (i) the violation is due to "circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the HIPAA provision violated," (ii) the violation is not due to willful neglect, and (iii) the violation is corrected during the applicable time period. For violations occurring on or	

[60] 78 Fed. Reg. at 5577, 5586; 45 C.F.R. § 160.410.
[57] 45 C.F.R. § 160.410(b) (2007).
[58] 74 Fed. Reg. at 56128 – 29.
[59] 75 Fed. Reg. at 40881.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		after February 18, 2009, the Proposed Rule adopted the Interim Final Rule's modified third defense and expanded it to apply to business associates.	
§ 160.418 – Penalty not exclusive	Generally, penalties may be imposed under the provisions of this part as well as any other applicable provision(s) of law. However, where a penalty has already been imposed under § 1177 of the Social Security Act, no additional penalty under these provisions is permitted.[61]	The Proposed Rule modified this section to include that penalties may not be imposed under both these provisions and § 299b-22(f) of the Patient Safety and Quality Improvement Act.[62]	Adopts as proposed.[63]
§ 160.420 – Notice of proposed determination	If a penalty is imposed in accordance with this part, the Secretary must deliver or send to the respondent a written notice of proposed determination.[64] This notice must include, among other things, the amount of the proposed penalty.[65]	The Interim Final Enforcement Rule required the Secretary to identify in the notice of proposed determination, in addition to the amount, the penalty tier on which the proposed penalty amount is based.[66]	Retains without modification.[67]
§ 160.534 – The hearing	In a hearing with an ALJ, the respondent has the burden of persuasion with respect to any: (i) affirmative defense;[68] (ii) challenge to the amount of the proposed penalty, including any mitigating factors;[69] or	The Interim Final Breach Notification Rule added that a respondent has the burden of persuasion with respect to demonstrating that all required breach notifications were made (or that a use or disclosure did not constitute a	Retains without modification.[73]

[61] 45 C.F.R. § 160.418 (2007) (referencing 42 U.S.C. § 1320d-5(b)(1)).
[62] 75 Fed. Reg. at 40881.
[63] 78 Fed. Reg. at 5586; 45 C.F.R. § 160.418.
[64] 45 C.F.R. § 160.420(a) (2007).
[65] 45 C.F.R. § 160.420(b) (referencing § 160.504, governing ALJ hearing requests).
[66] 74 Fed. Reg. 56129.
[67] 78 Fed. Reg. at 5586; 45 C.F.R. § 160.420(a)(4).
[68] 45 C.F.R. § 160.534(b)(1)(i) (2007) (referencing § 160.410, governing affirmative defenses).
[69] 45 C.F.R. § 160.534(b)(1)(ii) (2007) (referencing §§ 160.404 – 160.408, governing penalties).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	(iii) claim that a proposed penalty should be reduced or waived.[70] The Secretary has the burden of persuasion with respect to all other issues, including issues of liability and the existence of any aggravating factors.[71]	breach). The Interim Final Rule further noted that the Secretary has the burden of persuasion with respect to all other issues except for issues of liability under the Breach Notification Rule.[72]	

[73] 78 Fed. Reg. at 5569; 45 C.F.R. § 160.534(b).
[70] 45 C.F.R. § 160.534(b)(1)(iii) (2007) (referencing § 160.412, governing reductions/waivers of proposed penalties).
[71] 45 C.F.R. § 160.534(b)(2) (2007).
[72] Breach Notification for Unsecured Protected Health Information; Interim Final Rule with Request for Comments, 74 Fed. Reg. 42740, at 42755 (August 24, 2009).