3.) **The Breach Notification Rule** (*Part 164, Subpart D*)

- § 164.400 – Applicability
- § 164.402 – Definitions (breach, unsecured protected health information)
- § 164.404 – Notification to individuals
- § 164.406 – Notification to the media
- § 164.408 – Notification to the Secretary
- § 164.410 – Notification by a business associate
- § 164.412 – Law enforcement delay
- § 164.414 – Administrative requirements and burden of proof

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.400 – Applicability	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule applied the requirements of subpart D (Notification in the Case of Breach of Unsecured Protected Health Information) to breaches of protected health information that occur on or after September 23, 2009.[1]	Retains without modification.[2]

[1] 74 Fed. Reg. at 42743.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.402 – Definitions, *breach*	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule defined *breach* as the access, acquisition, use, or disclosure of protected health information in a manner that is not permitted by the Privacy Rule, which "compromises the security or privacy of the protected health information." Information is compromised if the "harm standard" is met, meaning that use or disclosure of the information poses a "significant risk of financial, reputational, or other harm to the individual." The use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2),[3] birth dates, or zip codes does not compromise the information. A "breach" excluded three types of uses and disclosures of protected health information: (i) any unintentional acquisition, access, or use by a workforce member or person acting on behalf of a covered entity or business associate, if it occurred in good faith and within the scope of the person's authority, and does not result in further use or disclosure in a manner not	The Final Rule modifies the definition of *breach*. It retains the Interim Final Rule's definition, but does not use the harm standard to define when information is compromised. Instead, an impermissible use or disclosure is presumed to be a breach unless the covered entity or business associate (as applicable) demonstrates that there is a low probability that the protected health information has been compromised, using a risk assessment based on at least four factors: (i) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the protected health information or to whom the disclosure was made; (iii) whether the protected health information was actually acquired or viewed; and (iv) the extent to which the risk to the protected health information has been mitigated.[5] The Final Rule retains all three exclusions from the definition of breach without modification.[6]

[2] 78 Fed. Reg. at 5566; 45 C.F.R. § 164.400.
[3] These include 16 different identifiers, such as names, social security numbers, telephone numbers, and IP addresses (45 C.F.R. § 164.514(e)(2) (2007)).
[5] 78 Fed. Reg. at 5641; 45 C.F.R. § 164.402, at ¶ (2) of "Breach."
[6] 78 Fed. Reg. at 5695; 45 C.F.R. § 164.402, at ¶ (1) of "Breach."

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		permitted under the Privacy Rule; (ii) any inadvertent disclosure by a person authorized to access protected health information to other authorized persons at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates, if the information received as a result of the inadvertent disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; and (iii) a disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not have been able to retain such information.[4]	
§ 164.402 – Definitions, *unsecured protected health information*	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule defined *unsecured protected health information* as protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.[7]	The Final Rule modifies *unsecured protected health information* by replacing "unauthorized individuals" with "unauthorized persons," because use of the term "individual," as it is defined in § 164.103, is not consistent with the meaning of this section.[8]
§ 164.404 – Notification to individuals	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule required covered entities, following discovery of a breach of unsecured protected health information,	Retains without modification.[10]

[4] 74 Fed. Reg. at 42743.
[7] 74 Fed. Reg. at 42743.
[8] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.402.
[10] 78 Fed. Reg. at 5647, 49; 45 C.F.R. § 164.404.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		to notify each individual whose information has been (or is reasonably believed to have been) "accessed, acquired, used, or disclosed as a result of such breach." A covered entity "discovers" a breach on the first day that it or any of its workforce members or agents (other than the person committing the breach), knew of the breach or would have known of the breach by exercising reasonable diligence. The notice must comply with requirements regarding: (1) timeliness (provided without unreasonable delay, and in no case later than 60 calendar days after discovery); (2) content (written in plain language, and including five specific pieces of information); (3) method of notice (written and either sent by first-class mail to the individual's last known address or if the individual agrees, by e-mail); and (4) method of notice if the covered entity knows the individual is deceased (written, by first-class mail to either the individual's next of kin or personal representative, if the covered entity has the address). Covered entities may issue multiple notices as they learn more about the breach.[9]	

[9] 74 Fed. Reg. at 42748-49.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		If the covered entity has insufficient or out-of-date contact information that precludes written notice as required, the covered entity must provide a substitute form of notice reasonably calculated to reach the individual (substitute notice is unnecessary if the individual is deceased). Where there is insufficient information for fewer than 10 individuals, substitute notice may be made "by an alternative form of written notice, telephone, or other means." Where there is insufficient information for 10 or more individuals, substitute notice must be made in either a conspicuous posting on the covered entity's home page for 90 days or in a conspicuous notice in major print or broadcast media available in the geographic area where the affected individuals reside. The notice must include a toll free number that will remain active for 90 days for individuals to call to receive more information. If the covered entity believes a situation is urgent because of possible imminent misuse of information, the covered entity may notify individuals by phone or other means, in addition to providing written notice as required.	
§ 164.406 – Notification to the media	The HIPAA rules reserved subpart D for future use, but do not include any	The Interim Final Breach Notification Rule required covered entities,	The Final Rule retains this section, but removes the reference to American

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	content therein.	following discovery of a breach involving more than 500 residents of a State (including American Samoa and the Northern Mariana Islands) or jurisdiction, to notify prominent media outlets serving the area without unreasonable delay but no later than 60 days after the discovery. Media notices must contain the same content as is required for individual notifications.[11]	Samoa and Northern Mariana Islands, which are now included in the definition of *State* in § 160.103.[12]
§ 164.408 – Notification to the Secretary	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule required covered entities to notify the Secretary following discovery of a breach. For a breach involving 500 or more individuals, covered entities must provide notice to the Secretary "contemporaneously" with notice to individuals. For breaches involving less than 500 individuals, covered entities must maintain a log or other documentation of such breaches, and provide notification to the Secretary of breaches occurring during the preceding calendar year, within 60 calendar days of the end of the year.[13]	The Final Rule retains this section, but modifies the provision governing notification to the Secretary of breaches involving less than 500 individuals, such that covered entities must annually notify the Secretary only of breaches **discovered** during the preceding calendar year.[14]
§ 164.410 – Notification by a business associate	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule required business associates to notify the covered entity following	Retains without substantive modification.[16]

[11] 74 Fed. Reg. at 42752.
[12] 78 Fed. Reg. at 5653; 45 C.F.R. § 164.406.
[13] 74 Fed. Reg. at 42753.
[14] 78 Fed. Reg. at 5654; 45 C.F.R. § 164.408.
[16] 78 Fed. Reg. at 5656; 45 C.F.R. § 164.410.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		discovery of a breach of unsecured protected health information. A business associate discovers a breach on the day that it or its employee, officer, or agent (other than the person committing the breach) knew of the breach or would have known of the breach by exercising reasonable diligence. The notice must comply with requirements regarding timeliness (without unreasonable delay and no later than 60 days after discovery), and content (identification of each individual whose information has been, or is reasonably believed to have been breached, and any other available information that the covered entity is required to include in its notification to the individual).[15]	
§ 164.412 – Law enforcement delay	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule required covered entities and business associates to delay breach notification if a law enforcement official states that releasing the information would impede a criminal investigation or threaten national security. If the statement is in writing, the delay must last as long as is specified. If the statement is made	Retains without modification.[18]

[15] 74 Fed. Reg. at 42753.
[18] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		orally, the covered entity or business associate must document the statement, include the identity of the requesting officer, and delay notification for up to 30 days from the date of the statement; if a written statement is submitted within the 30 day time period, the notification must be delayed for as long as the written statement specifies.[17]	
§ 164.414 – Administrative requirements and burden of proof	The HIPAA rules reserved subpart D for future use, but do not include any content therein.	The Interim Final Breach Notification Rule required covered entities to comply with the administrative requirements of § 164.530 regarding training, complaints, intimidation and retaliation, waiver of rights, policies and procedures, and documentation. Covered entities and business associates have the burden of demonstrating their compliance with all applicable notice requirements, or demonstrating that a use or disclosure was not a breach.[19]	Retains without modification.[20]

[17] 74 Fed. Reg. at 42755.
[19] 74 Fed. Reg. at 42755.
[20] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.414.