A Side-by-Side Table Comparing the Administrative Simplification Regulations to the Changes in the Proposed, Interim Final, and Final Omnibus Rules Implementing HITECH, GINA, and PSQIA

Health Information and the Law[1]
The George Washington University Department of Health Policy

February 14, 2013

Background

The 1996 HIPAA statute required the Secretary of the U.S. Department of Health and Human Services (HHS) to publish regulations implementing HIPAA's Administrative Simplification provisions. From 2000 through 2004, the Secretary released five regulations (the Administrative Simplification regulations, or "Rules"), satisfying this requirement.1 HHS' Office of Civil Rights (OCR) oversees compliance with the Security and Privacy Rules, while HHS' Centers for Medicare & Medicaid Services (CMS) oversees compliance with the Transaction and Code Sets and Unique Identifiers Rule. Both OCR and CMS conduct their oversight in accordance with the provisions of the Enforcement Rule.

Several laws have modified or expanded the original HIPAA requirements, necessitating changes to all five Rules. HITECH (of 2009) required changes to the Privacy, Security, and Enforcement Rules, and mandated the adoption of a sixth Rule – the Breach Notification Rule – to be overseen by OCR in accordance with the HITECH-modified provisions of the Enforcement Rule. GINA (of 2008) and PSQIA (of 2005) also made changes to the Privacy Rule. To comply with these requirements, the Secretary issued four separate rulemakings in 2009 and 2010 that made the changes required by HITECH, GINA, and PSQIA:

[1] Health Information & the Law (www.HealthInfoLaw.org) is a project of the George Washington University School of Public Health and Health Services' Hirsh Health Law and Policy Program developed with support from the Robert Wood Johnson Foundation. The project is designed to serve as a practical online resource to federal and state laws governing access, use, release, and publication of health information. Regularly updated, the website addresses the current legal and regulatory framework of health information law and changes in the legal and policy landscape impacting health information law and its implementation.

- Interim Final Rule issued on August 24, 2009 creating the Breach Notification Rule as required by HITECH.
- Proposed Rule issued on October 7, 2009 modifying the Privacy Rule as required by GINA.
- Interim Final Rule issued on October 30, 2009 modifying the Enforcement Act as required by HITECH.
- Proposed Rule issued on July 14, 2010 implementing the PSQIA requirement and the remaining HITECH requirements, modifying the Privacy, Security and Enforcement Rules.

On January 17, 2013, HHS released a Final Omnibus Rulemaking finalizing amendment of several sections of the Privacy, Security, Breach Notification and Enforcement Rules in accordance with these four rulemakings. The Final Rule will be effective on March 26, 2013; covered entities must be in compliance with the updated provisions as modified by the Final Rule by September 23, 2013.

This side-by-side table compares every provision of the Proposed/Interim Final Rules with the relevant sections of the HIPAA Administrative Simplification regulations as they originally existed, and with the updated provisions of the Final Omnibus Rule. Also available at healthinfolaw.com are an overview highlighting the most significant differences between the proposed and final rules and a section-by-section analysis giving a detailed description of both the proposed and finalized changes, as well as relevant comments received and HHS' response.

Table of Contents

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.500 – Applicability	The provisions of the Privacy Rule apply to covered entities with respect to protected health information, with some exceptions for health care clearinghouses.[2]	The Proposed Rule added a provision noting that, where provided, the provisions of the Privacy Rule apply to business associates with respect to protected health information of a covered entity.[3]	Adopts as proposed.[4]
§ 164.501 – Definitions, *health care operations*	*Health care operations* include six separate groups of activities carried out by a covered entity, to the extent that the activities are related to covered functions.[5] The third activity group includes "underwriting, premium rating, and other activities conducted by a covered entity relating to the creation, renewal or replacement of a contract of health insurance or health benefits..."[6]	The Proposed Rule added "patient safety activities" to the first group of health care operations activities.[7] The Proposed GINA Rule amended the third activity group by removing "underwriting" and adding the term "enrollment."[8]	The Final Rule adopts the Proposed Rule's addition.[9] The Final Rule does not remove the term "underwriting," but adds a reference to the underwriting prohibition at § 164.502(a)(5)(i) to the third activity group; the Final Rule retains the addition of the term "enrollment."[10]
§ 164.501 – Definitions, *marketing*	The first paragraph of *marketing* includes "making a communication about a product or service that encourages recipients to purchase or use the product or service." Three types of communications are excluded from this definition, and include	The Proposed Rule retained the first paragraph of *marketing*, but modified the excluded communications. The Proposed Rule combined the second and third exceptions into one exception that only applies when a health care provider is making the communication.	The Final Rule retains the proposed changes to *marketing*, with two modifications. The exception combining the second and third exceptions is moved so that it will also be considered *marketing* if the covered entity receives financial remuneration

[2] 45 C.F.R. § 164.500 (2007).
[3] 75 Fed. Reg. at 40883-84.
[4] 78 Fed. Reg. at 5695; 45 C.F.R. § 164.500(c).
[5] 45 C.F.R. § 164.501, at "Health care operations" (2007).
[6] 45 C.F.R. § 164.501, at ¶ (3) of "Health care operations" (2007).
[7] 75 Fed. Reg. at 40884.
[8] 74 Fed. Reg. at 51703.
[9] 78 Fed. Reg. at 5592; 45 C.F.R. § 164.501, at ¶ (1) of "Health care operations."
[10] 78 Fed. Reg. at 5666; 45 C.F.R. § 164.501, at ¶ (3) of "Health care operations."

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	communications made: (i) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication; (ii) for treatment of the individual; or (iii) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. [11] The second paragraph of *marketing* includes the disclosure of protected health information from a covered entity to a third party, in exchange for direct or indirect remuneration, for use by the third party or its affiliate in marketing its own product or service.[12]	The Proposed Rule added a qualification to this exclusion, so that if such communication is in writing and the provider receives financial remuneration, it is not *marketing* only if the requirements of § 164.514(f)(2) are met. The Proposed Rule added an additional exclusion for refill reminders or other communications about a current prescription if the financial remuneration the covered entity receives (if any) is limited to those costs that are reasonably related to the cost of making the communication. The Proposed Rule retained the first exclusion and added an additional exclusion: "contacting individuals with information about treatment alternatives for case management or care coordination and related functions to the extent these activities do not fall within the definition of treatment." The Proposed Rule added that these two exclusions **will** be considered *marketing* if the covered entity receives financial remuneration in exchange for making the communication.[13]	in exchange for making the communication. The Final Rule also removes the proposed qualification to this exclusion.[16]

[11] 45 C.F.R. § 164.501, at ¶ (1) of "Marketing" (2007).
[12] 45 C.F.R. § 164.501, at ¶ (2) of "Marketing" (2007).
[13] 75 Fed. Reg. at 40885-86.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		The Proposed Rule removed the second paragraph defining *marketing* as the disclosure of information for use by a third party in its own marketing.[14] The Proposed Rule defined *financial remuneration* as "direct or indirect payment from or on behalf of a third party whose product or service is being described." Such payment does not include any payment for treatment.[15]	
§ 164.501 – Definitions, *underwriting purposes*	The HIPAA rules do not define *underwriting purposes*.	The Proposed GINA Rule defined *underwriting purposes* with respect to a health plan as: (i) rules governing benefit determinations/eligibility for benefits, or the determination of benefits/eligibility for benefits (including enrollment, continued eligibility, and changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (ii) premium or contribution calculations (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or	The Final Rule adopts the proposed definition of *underwriting purposes*, but moves it to § 164.502(a)(5)(i), which is referred to as "the underwriting prohibition."[18]

[16] 78 Fed. Reg. at 5595-97; 45 C.F.R. § 164.501, at "Marketing."
[14] 75 Fed. Reg. at 40887.
[15] 75 Fed. Reg. at 40885.
[18] 78 Fed. Reg. at 5665; 45 C.F.R. § 164.502(a)(5)(i).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		participating in a wellness program); (iii) the application of any preexisting condition exclusion; and (iv) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. The definition excludes determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.[17]	
§ 164.501 – Definitions, *payment*	*Payment* means the activities undertaken by: (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits; or (ii) a health care provider or health plan to obtain or provide reimbursement for the provision of health care.[19]	The Proposed GINA Rule added a reference to the underwriting prohibition to the definition of *payment*.[20]	Adopts as proposed.[21]
§ 164.502 – Uses and disclosures of protected health information: general rules	This section identifies ten standards governing the general use or disclosure of protected health information, which apply to covered entities. The first standard prohibits a covered entity from using or disclosing protected health information, except as is permitted or required.[22] The standard	The Proposed Rule applied the first standard to business associates, but did not apply the provisions listing the permitted or required disclosures, and changed the titles of those provisions to make clear that they apply only to covered entities.[29] The Proposed Rule added two provisions to the first standard. The first identifies the uses or	The Final Rule adopts the Proposed Rule's modifications to the first standard, with minor technical modifications.[36] The Final Rule adopts the Proposed GINA Rule's inclusion of an underwriting prohibition within the first standard, but modifies the

[17] 74 Fed. Reg. at 51702-03.
[19] 45 C.F.R. § 164.501, at ¶ (1) of "Payment" (2007).
[20] 74 Fed. Reg. at 51703.
[21] 78 Fed. Reg. at 5666; 45 C.F.R. § 164.501, at ¶(1)(i) of "Payment."
[22] 45 C.F.R. § 164.502(a) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	includes a provision listing six permitted disclosures, and a provision listing two required disclosures. The second standard requires that, when using or disclosing protected health information (or when requesting such information from another covered entity), a covered entity must make reasonable efforts to limit such information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[23] The minimum necessary standard does not apply to six specific uses and/or disclosures. The fifth standard applies to covered entities that choose to disclose protected health information to a business associate and/or allow a business associate to create or receive protected health information on its behalf, and requires such covered entities to obtain satisfactory assurances that its business associate will appropriately safeguard information.[24] This standard does not	disclosures a business associate is permitted to make (only as permitted or required by its contract or other arrangement or as required by law). A business associate is prohibited from uses or disclosures that would violate the Privacy Rule if done by the covered entity, except for the purposes specified in § 164.504(e)(2)(i)(A) or (B).[30] The second added provision identified two disclosures a business associate is required to make (when required by the Secretary under the Enforcement Rule and to the covered entity, individual, or individual's designee, as necessary to satisfy the covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii)).[31] The Proposed GINA Rule added a provision to the first standard that prohibits health plans from using or disclosing protected health information that is genetic information for underwriting purposes.[32] The Proposed Rule applied the second standard to business associates to the	language to exclude issuers of long-term care policies, and moves the definition of "underwriting purposes" as proposed by the GINA rule at § 164.501 to this standard, which is referred to as "the underwriting prohibition."[37] The Final Rule also adds a general prohibition on the sale of protected health information by a covered entity or business associate, except where the covered entity obtains an authorization in accordance with § 164.508(a)(4).[38] The Final Rule defines *sale of protected health information* as a disclosure of protected health information by a covered entity or business associate in exchange for direct or indirect remuneration from or on behalf of the recipient.[39] The Final Rule moves exceptions to *sale of protected health information* from proposed § 164.508(a)(4)(ii) to this provision.[40] The Final Rule adopts the modifications to the second,[41] fifth,[42]

[29] 75 Fed. Reg. at 40887.
[36] 78 Fed. Reg. at 5598; 45 C.F.R. § 164.502(a).
[23] 45 C.F.R. § 164.502(b)(1) (2007).
[24] 45 C.F.R. § 164.502(e)(1)(i) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	apply to three specific uses and/or disclosures.[25] A business associate that is itself a covered entity will be held responsible for complying with this standard, and with § 164.504(e), as a covered entity.[26] A covered entity must document the required satisfactory assurances through a written contract or other agreement/arrangement with the business associate that meets the requirements of § 164.504(e).[27] The sixth standard requires covered entities to comply with the Privacy Rule with respect to protected health information of a deceased individual.[28]	same extent it applies to covered entities.[33] The Proposed Rule modified the fifth standard by specifying that a covered entity is not required to obtain assurances from a subcontractor, and adding a provision requiring a business associate to obtain satisfactory assurances that a subcontractor will appropriately safeguard information. The Proposed Rule removed the provision excluding three specific uses/disclosures (and relocated these exclusions to the revised definition of "business associate" at § 160.103). It also removed the provision holding a business associate responsible for	and sixth standards[43] as proposed.

[30] This section governs uses and disclosures for organizational requirements; these provisions permit the use and disclosure of protected health information for the proper management and administration of the business associate, or to provide data aggregation services relating to the health care operations of the covered entity (45 C.F.R. § 164.504(e)(2)(i)(A), (B) (2007)).
[31] 75 Fed. Reg. at 40887.
[32] 74 Fed. Reg. at 51703-04.
[37] 78 Fed. Reg. at 5666-67; 45 C.F.R. § 164.502(a)(5)(i).
[38] 78 Fed. Reg. at 5606; 45 C.F.R. § 164.502(a)(5)(ii)(A).
[39] 78 Fed. Reg. at 5606; 45 C.F.R. § 164.502(a)(5)(ii)(B)(1).
[40] 78 Fed. Reg. at 5606; 45 C.F.R. § 164.502(a)(5)(ii)(B)(2) (the Proposed Rule describes these exceptions at 75 Fed. Reg. at XX).
[41] 75 Fed. Reg. at 5599; 45 C.F.R. § 164.502(b)(1).
[42] 75 Fed. Reg. at 5601; 45 C.F.R. § 164.502(e).
[25] 45 C.F.R. § 164.502(e)(1)(ii) (2007).
[26] 45 C.F.R. § 164.502(e)(1)(iii) (2007).
[27] 45 C.F.R. § 164.502(e)(2) (2007).
[28] 45 C.F.R. § 164.502(f) (2007).
[33] 75 Fed. Reg. at 40887 – 88.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		compliance with this standard as a covered entity.[34] The Proposed Rule applied the documentation requirement to business associates in the same manner as it applies to covered entities. The Proposed Rule modified the sixth standard such that it no longer applies 50 years after the death of the individual.[35]	
§164.504 – Uses and disclosures: Organizational requirements	This section identifies three organizational requirement standards that covered entities must satisfy. The first standard sets forth the requirements for business associate contracts and other arrangements.[44] 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 certain steps to deal with the violation.[45] If such steps are unsuccessful, the covered entity must terminate the contract if feasible;[46] if termination is not feasible, the covered	The Proposed Rule made several modifications to the first standard. It removed the provision requiring a covered entity to report to the Secretary if termination of the contract or arrangement is not feasible.[56] It added a provision requiring business associates to deal with material breaches or violations by its subcontractors in the same manner as covered entities are required to deal with breaches or violations by their business associates.[57] The Proposed Rule made the following modifications to the requirements a business associate must agree to meet: expanded requirement	Adopts the Proposed Rule's modifications.[61] The Final Rule adds that a covered entity satisfies the "business associate contract" standard and § 164.314(a)(1) if it discloses only a limited data set for the business associate to carry out a health care operations function and it has a data use agreement that complies with § 164.514(e)(4), and § 164.314(a)(1), if applicable. Adopts the Proposed GINA Rule's modifications.[62]

[43] 75 Fed. Reg. at 5614; 45 C.F.R. § 164.502(f).
[34] 75 Fed. Reg. at 40888.
[35] 75 Fed. Reg. at 40894-95.
[44] 45 C.F.R. § 164.504(e)(1)(i) (2007).
[45] 45 C.F.R. § 164.504(e)(1)(ii) (2007).
[46] 45 C.F.R. § 164.504(e)(1)(ii)(A) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	entity must report the problem to the Secretary.[47] A covered entity with a business associate contract satisfies the "business associate contract" standard when the contract includes three specific provisions, including that the business associate agrees to satisfy nine requirements.[48] Some of these requirements include: (B) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;[49] (C) report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;[50] and (D) ensure that any agents to whom the business associate provides protected health information it receives from a covered entity or that it creates or receives on behalf of the covered entity, agree to the same restrictions and conditions	(B), such that a business associate must comply with the Security Rule where applicable; added to requirement (C), specifying that business associates must report breaches of unsecured protected health information as required; and modified requirement (D) to "ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information."[58] The Proposed Rule added a tenth requirement that a business associate must agree to satisfy: "to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, [the business associate must] comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of	

[56] 75 Fed. Reg. at 40888.
[57] 75 Fed. Reg. at 40888 – 89.
[61] 78 Fed. Reg. at 5601; 45 C.F.R. § 164.504(e).
[62] 78 Fed. Reg. at 5667; 45 C.F.R. § 164.504(f)(1)(ii).
[47] 45 C.F.R. § 164.504(e)(1)(ii)(B) (2007).
[48] 45 C.F.R. § 164.504(e)(2) (2007).
[49] 45 C.F.R. § 164.502(e)(2)(ii)(B) (2007).
[50] 45 C.F.R. § 164.504(e)(2)(ii)(C) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	that apply to the business associate with respect to such information.[51] If a covered entity and its business associate are both governmental entities and have an arrangement other than a business associate contract, the covered entity satisfies the "business associate contract" standard: (A) by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of the three required contract provisions; or (B) when other law contains requirements applicable to the business associate that accomplish the objectives of the required provisions.[52] If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a "business associate service" to a covered entity, the covered entity may disclose protected health information to the extent necessary to comply with the legal mandate without meeting the requirements of the "business associate contract" standard,	such obligation." The Proposed Rule modified the "other arrangement" requirement applicable to government entities, such that the covered entity also satisfies § 164.314(a)(1) if the memorandum of understanding or other law accomplishes the objectives of the required contract provisions and the objectives of 164.314(a)(2), if applicable. The Proposed Rule modified the provision applicable when a business associate is required by law to perform a function or activity on behalf of a covered entity, such that a covered entity also need not meet the requirements of § 164.314(a)(1) if it attempts in good faith to obtain satisfactory assurances as required by both this section and § 164.314(a)(1), and properly documents the attempt and reasons the assurances cannot be obtained.[59] The Proposed Rule added a provision applying the requirements of §	

[58] 75 Fed. Reg. at 40889.
[51] 45 C.F.R. § 164.504(e)(2)(ii)(D) (2007).
[52] 45 C.F.R. § 164.504(e)(3)(i) (2007).
[59] 75 Fed. Reg. at 40888-89.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	if the covered entity attempts in good faith to obtain satisfactory assurances, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.[53] The second standard sets forth requirements for group health plans and issuers.[54] The group health plan may disclose summary health information to the plan sponsor when the plan sponsor requests such information for one of two specific purposes.[55]	164.504(e)(2) through (e)(4) to the contract or other arrangement between a business associate and its subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. The Proposed GINA Rule added a reference to the underwriting prohibition such that group health plans and issuers may not disclose genetic information that is protected health information for underwriting purposes when disclosing summary health information to a plan sponsor.[60]	
§ 164.506 – Uses and disclosures to carry out treatment, payment, or health care operations	This section describes the uses and disclosures a covered entity is permitted to make to carry out treatment, payment, or health care operations; this section does not apply to uses or disclosures that require an authorization.[63] One of the permitted uses and disclosures applies when a covered entity participates in an organized health care arrangement, in which case	The Proposed GINA Rule added a reference to the underwriting prohibition to make clear that covered entities may not use or disclose protected health information that is genetic information for underwriting purposes, even if such a use or disclosure is considered payment or health care operations.[65] The Proposed Rule modified the circumstances in which a covered	Adopts the Proposed GINA Rule's modification.[67] Adopts the Proposed Rule's modification.[68]

[53] 45 C.F.R. § 164.504(e)(3)(ii) (2007).
[54] 45 C.F.R. § 164.504(f)(1)(i) (2007).
[55] 45 C.F.R. § 164.504(f)(1)(ii) (2007).
[60] 74 Fed. Reg. at 51704.
[63] 45 C.F.R. § 164.506(a) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	such covered entity may disclose information to another covered entity that participates in the organized health care arrangement for any of the organized health care arrangement's health care operations activities.[64]	entity that participates in an organized health care arrangement may disclose protected health information about an individual, such that the covered entity may disclose the information to "other participants" in the arrangement. This change reflects the fact that entities other than covered entities participate in organized health care arrangements.[66]	
§ 164.508 – Uses and disclosures for which authorization is required	This section prohibits uses or disclosures of protected health information without a valid authorization, unless such use or disclosure is otherwise permitted under the Privacy Rule.[69] With limited exceptions, authorizations are required for the use or disclosure of psychotherapy notes[70] and for the use or disclosure of information for marketing.[71] The section identifies the elements of a valid authorization,[72] and	The Proposed Rule required covered entities to obtain an authorization for the sale of protected health information. The authorization must state that the covered entity will receive remuneration in exchange for disclosing the protected health information.[76] The Proposed Rule added exceptions to this requirement. Covered entities do not need to obtain an authorization to sell protected health information for: (A) public health purposes; (B) research purposes, where	The Final Rule notes that the requirement for covered entities to obtain an authorization for the sale of protected health information does not apply as provided by the transition provisions in § 164.532. The Final Rule modifies proposed exception (E) so that it also applies to disclosure of protected health information to or by a subcontractor for activities it undertakes on behalf of a business associate. The Final Rule then moves all eight proposed exceptions (as

[65] 74 Fed. Reg. at 51704.
[67] 78 Fed. Reg. at 5667; 45 C.F.R. § 164.506(a).
[68] 78 Fed. Reg. at 5698; 45 C.F.R. § 164.506(c)(5).
[64] 45 C.F.R. § 164.508(c)(5) (2007).
[66] 75 Fed. Reg. at 40904.
[69] 45 C.F.R. § 164.508(a)(1) (2007).
[70] 45 C.F.R. § 164.508(a)(2) (2007).
[71] 45 C.F.R. § 164.508(a)(3) (2007).
[72] 45 C.F.R. § 164.508(b)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	lists five defects that make an authorization invalid.[73] An authorization for a research study may be combined with any other type of written permission for the same research study, including another authorization for such research or a consent to participate in such research.[74] An authorization (other than for the use or disclosure of psychotherapy notes) may be combined with any other authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.[75]	the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the information; (C) for treatment and payment purposes; (D) for the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence; (E) to or by a business associate for activities that it undertakes on behalf of a covered entity, if the only remuneration provided is by the covered entity to the business associate for the performance of such activities;[77] (F) to the individual, when requested;[78] (G) as required by law; and (H) permitted by and in accordance with the applicable requirements of the Privacy Rule, where the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the information for such purpose, or a fee otherwise expressly permitted by law.[79]	modified) to § 164.502(a)(5)(ii) as exclusions from the definition of *sale of protected health information*.[83] The Final Rule adopts all other proposed modifications.[84]

[76] 75 Fed. Reg. at 40890 – 91.
[73] 45 C.F.R. § 164.508(b)(2) (2007).
[74] 45 C.F.R. § 164.508(b)(3)(i) (2007).
[75] 45 C.F.R. § 164.508(b)(3)(iii) (2007).
[77] 75 Fed. Reg. at 40891.
[78] 75 Fed. Reg. at 40891 - 92.
[79] 75 Fed. Reg. at 40892.
[83] 78 Fed. Reg. at 5606 - 07; 45 C.F.R. § 164.508(a)(4) (see exceptions and general prohibition on the sale of protected health information at 45 C.F.R. § 164.502(a)(5)(ii)(B)).
[84] 78 Fed. Reg. at 5610 - 11; 45 C.F.R. § 164.508(b)(3).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		The Proposed Rule modified the provision permitting covered entities to combine authorizations for the use or disclosure of protected health information for research purposes. The Proposed Rule added that an authorization for a research study may be combined with an authorization for the creation or maintenance of a research database or repository.[80] It also added that where a covered health care provider conditions the provision of research-related treatment on the provision of an authorization, any compound authorization must clearly differentiate between the conditioned and unconditioned components, and allow the individual to opt in to activities described in the unconditioned authorization.[81] The Proposed Rule also modified the provision permitting compound authorizations except where the covered entity has conditioned treatment, payment, enrollment or eligibility on provision of one of the authorizations. The Proposed Rule adds that this prohibition does not apply to a	

[80] 75 Fed. Reg. at 40892.
[81] 75 Fed. Reg. at 40893.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		compound authorization created for research purposes as described.[82]	
§ 164.510 – Uses and disclosures requiring an opportunity for the individual to agree or to object	This section sets forth uses and disclosures about which an individual must be informed in advance and given an opportunity to agree or to prohibit or restrict the use or disclosure.[85] Except when an objection is expressed, a covered health care provider may disclose certain protected health information for facility directory purposes.[86] A covered entity may disclose protected health information about an individual to his or her relative, close personal friend, or any other person he or she identifies, to the extent that such information is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care,[87] or as is needed to notify such person about the individual's location, general condition, or death.[88] Prior to the disclosure, the covered entity must	The Proposed Rule added that a covered health care provider may also **use** information for directory purposes.[90] The Proposed Rule adds that when an individual is not present (or an opportunity to agree or object cannot practicably be provided), a covered entity may also disclose information to the extent that it is directly relevant to the person's involvement with payment related to the individual's health care or as needed for notification purposes.[91] The Proposed Rule adds an new provision such that if an individual is deceased, a covered entity may disclose information to the individual's relative, close personal friend, or other person identified by the individual who was involved in the individual's care or payment for health care prior to the individual's death. A covered entity may not provide such information if it	Adopts as proposed.[93]

[82] 75 Fed. Reg. at 40892.
[85] 45 C.F.R. § 164.510 (2007).
[86] 45 C.F.R. § 164.510(a)(1)(ii) (2007).
[87] 45 C.F.R. § 164.508(b)(1)(i) (2007).
[88] 45 C.F.R. § 164.508(b)(1)(ii) (2007).
[90] 75 Fed. Reg. at 40904.
[91] 75 Fed. Reg. at 40904.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	obtain the individual's agreement to the disclosure, provide the individual an opportunity to object, or reasonably infer that the individual does not object. If the individual is not present (or the opportunity to agree or object cannot practicably be provided), the covered entity may only disclose protected health information to the extent that it is directly relevant to the person's involvement with the individual's health care if it determines that such disclosure is in the individual's best interests.[89]	knows that the individual had expressed that he or she did not want such information disclosed.[92]	
§ 164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required	This section sets forth the situations in which a covered entity may use or disclose protected health information without obtaining an authorization or providing an opportunity for the individual to agree or object.[94] Among other purposes, a covered entity may disclose protected health information to certain entities for public health activities and purposes.[95]	The Proposed Rule added that a covered entity may disclose proof of immunization information to a school about an individual who is a student or prospective student at such school, if a the law requires the school to have such proof prior to admitting the individual. The covered entity must first obtain agreement to the disclosure from the individual (if the individual is an adult or emancipated minor), or from the individual's parent, guardian, or other person legally acting in place of the individual's parent..[96]	The Final Rule adopts the Proposed Rule's modifications, but requires that the covered entity to document the consent to the disclosure.[97]

[93] 78 Fed. Reg. at 5615; 45 C.F.R. § 164.510.
[89] 45 C.F.R. § 164.510(b)(3) (2007).
[92] 75 Fed. Reg. at 40895.
[94] 45 C.F.R. § 164.512 (2007).
[95] 45 C.F.R. § 164.512(b)(1) (2007).
[96] 75 Fed. Reg. at 40895.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.514 – Other requirements relating to uses and disclosures of protected health information	This section sets forth requirements for several uses and disclosures of protected health information not discussed in other sections. A covered entity may, without an authorization and for the purpose of raising funds for its own benefit, use or disclose to a business associate or to an institutionally related foundation the following information: demographic information relating to an individual, and dates of health care provided to an individual.[98] There are three requirements a covered entity must follow to comply with the fundraising standard: (1) include a statement as required in §164.520(b)(1)(iii)(B) in its notice;[99] (2) include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving any further fundraising communications;[100] and (3) make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.[101]	The Proposed Rule modified the requirements a covered entity must follow to comply with the fundraising authorization provision: (1) include in its notice of privacy practices a statement that it may contact individuals to raise funds for the covered entity as required by § 164.520(b)(1)(iii)(A); (2) in each fundraising communication sent to an individual, provide the individual with "a clear and conspicuous opportunity" to opt out of receiving future fundraising communications. The opt-out method may not cause the individual to incur an undue burden or more than a nominal cost; and (3) where the individual has opted out, the covered entity is prohibited from sending fundraising communications. The Proposed Rule adds a fourth requirement prohibiting covered entities from conditioning provision of treatment or payment on an individual's decision to opt in or out of fundraising communications.[103] The Proposed Rule also added an	The Final Rule adopts the proposed fundraising provision and adds that the covered entity may also use or disclose the following information: department of service information, treating physician, outcome information, and health insurance status, and that demographic information relating to an individual may include name, address, other contact information, age, gender, and date of birth.[106] The Final Rule adds a fifth provision allowing a covered entity to provide an individual who has elected not to receive further fundraising communications with a method to opt back in.[107] The Final Rule does not adopt the proposed inclusion of an exception for uses and disclosures for remunerated treatment communications.[108] The Final Rule does not adopt the Proposed GINA rule's suggested title change or removal of the term "underwriting," but does adopt the reference to the underwriting prohibition as proposed.[109]

[97] 78 Fed. Reg. at 5617; 45 C.F.R. § 164.512(b)(vi).
[98] 45 C.F.R. § 164.514(f)(1) (2007).
[99] 45 C.F.R. § 164.514(f)(2)(i) (2007).
[100] 45 C.F.R. §164.514(f)(2)(ii) (2007).
[101] 45 C.F.R. § 164.514(f)(2)(iii) (2007).
[103] 75 Fed. Reg. at 40896-97.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	A health plan that receives protected heath information about an individual for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, but that does not include the insurance or benefits within the plan, may only use or disclose such information as required by law.[102]	exception for uses and disclosures for remunerated treatment communications if certain requirements are met.[104] The Proposed GINA Rule modified the standard for uses and disclosures for underwriting and related purposes by changing the title of the standard to "uses and disclosures for activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits," removing the term "underwriting," and adding that the exception for a use or disclosure as required by law is subject to the underwriting prohibition.[105]	
§ 164.520 – Notice of privacy practices for protected health information	An individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity and of the individual's rights and the covered entity's legal duties with respect to such information.[110] This section identifies the content that	The Proposed Rule modified some of the provisions describing the required content of the notice. In addition to the required statements that other uses and disclosures require authorization and that individuals may revoke an authorization, covered entities must describe the types of uses and disclosures that require an	The Final Rule adopts most of the Proposed Rule's modifications to the content requirements, but omits statement (A) (both the proposed modification and the original).[120] The Final Rule accepts the Proposed GINA Rule's addition of a statement about underwriting purposes, but adds

[106] 78 Fed. Reg. at 5622; 45 C.F.R. § 164.514(f).
[107] 78 Fed. Reg. at 5621; 45 C.F.R. § 164.514(f)(2)(v).
[108] 78 Fed. Reg. at 5596.
[109] Final Rule, p. 411.
[102] 45 C.F.R. § 164.514(g) (2007).
[104] 75 Fed. Reg. at 40884 – 86.
[105] 74 Fed Reg 51704 (2009).
[110] 45 C.F.R. § 164.520(a)(1) (2007).
[120] 78 Fed. Reg. at 5624 - 25; 45 C.F.R. § 164.520(b)(1).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	must be included in the notice. The notice must describe the uses and disclosures the covered entity is permitted or required to make for treatment, payment, and health care operations,[111] and for all other purposes without the individual's written authorization.[112] The notice must include the following statements: uses and disclosures [other than those specified] require the individual's written authorization, and the individual may revoke such authorization as provided by § 164.508(b)(5).[113] If a covered entity intends to engage in certain activities, it must include a separate statement to that effect (within the description of the types of uses and disclosures the entity is permitted to make for treatment, payment, and health care operations), as applicable. The statements include: (A) the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may	authorization. The Proposed Rule modified the provision requiring a covered entity to inform individuals if it intends to engage in certain activities. Statement (A) is modified so that it only applies to health care providers, who must inform the individual (as applicable) that they may send communications "concerning treatment alternatives or other health-related products or services," for which the provider receives financial remuneration, and that the individual has the right to opt-out of receiving such communications. Statement (B) is modified so that the covered entity must state that the individual has a right to opt out of receiving [fundraising] communications.[118] The Proposed GINA Rule also modified this provision by adding that if a covered health plan intends to use or disclose protected health information for underwriting purposes, it must include in their notice statement (D): the covered entity is prohibited	that the provision does not apply to issuers of long-term care policies.[121] The Final Rule also modifies the provision requiring a description of the covered entity's duties, by adding that a covered entity must include in the statement about its legal duties that it is required to notify affected individual's following a breach of unsecured protected health information.[122] The Final Rule adds a new paragraph within the requirements for health plans. When there is a material change to the notice, a health plan that currently post its notice on its web site must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.[123] A health plan that does not post its notice on a web site must provide the revised notice, or information about the material change

[111] 45 C.F.R. § 164.520(b)(1)(ii)(A) (2007).
[112] 45 C.F.R. § 164.520(b)(1)(ii)(B) (2007).
[113] 45 C.F.R. § 164.520(b)(1)(ii)(E) (2007).
[118] 75 Fed. Reg. at 40897-98.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	be of interest to the individual; (B) the covered entity may contact the individual to raise funds for the covered entity; or (C) a group health plan or issuer may disclose protected health information to the sponsor of the plan.[114] The notice must describe the individual's rights with respect to protected health information and how the individual may exercise these rights, including the right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction.[115] The notice must also describe the covered entity's duties, including a statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with	from using or disclosing protected health information that is genetic information of an individual for underwriting purposes.[119] Within the provision requiring a statement of the individual's right to request restrictions, the Proposed Rule modified the statement that a covered entity is not required to agree to a requested restriction by adding that it must agree to such request when the is disclosure restricted under §164.522(a)(1).	and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.[124]

[121] 78 Fed. Reg. at 5668; 45 C.F.R. § 164.520(b)(1)(iii)(C).
[122] 78 Fed. Reg. at 5624 -25; 45 C.F.R. § 164.520(b)(1)(v)(A).
[123] 78 Fed. Reg. at5625; 45 C.F.R. § 164.520(c)(1)(v)(A).
[114] 45 C.F.R. § 164.520(b)(1)(iii) (2007).
[115] 45 C.F.R. § 164.520(b)(iv)(A) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	respect to protected health information.[116] This section also sets forth requirements governing provision of notice, including specific requirements for health plans.[117]		
§ 164.522 – Rights to request privacy protection for protected health information	A covered entity must permit an individual to request that the covered entity restrict the use or disclosure of the individual's protected health information for purposes of treatment, payment, or health care operations, or for involvement in the individual's care, payment for care, or notification.[125] A covered entity is not required to agree to a [requested] restriction.[126] If a covered entity does choose to agree to a restriction, it must comply with certain requirements.[127] A covered entity may terminate its agreement to a restriction if it meets certain requirements, including informing the individual that it is terminating its agreement to a restriction, and noting that such	The Proposed Rule adds a provision to this section requiring covered entities to agree to an individual's request to restrict disclosure of his or her protected health information to a health plan if: (A) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (B) the information pertains solely to a health care service or item paid for in full by either the individual or a third party on behalf of the individual other than the health plan. The Proposed Rule also modified the provision governing termination of a restriction, such that when the covered entity informs the individual that it is terminating its agreement to a	Adopts as proposed.[130]

[119] 74 Fed. Reg. at 51704.
[124] 78 Fed. Reg. at 5625; 45 C.F.R. § 164.520(c)(1)(v)(B).
[116] 45 C.F.R. § 164.520(b)(1)(v)(A) (2007).
[117] 45 C.F.R. § 164.520(c)(1) (2007).
[125] 45 C.F.R. § 164.522(a)(1)(i) (2007).
[126] 45 C.F.R. § 164.522(a)(1)(ii) (2007).
[127] 45 C.F.R. § 164.522(a)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	termination only applies to protected health information created or received after it has so informed the individual.[128]	restriction, it must also note that such termination does not apply to information it is required to restrict (i.e., to a health plan as described above).[129]	
§ 164.524 – Access of individuals to protected health information	An individual has the right, with limited exceptions, to inspect and obtain a copy of his or her protected health information that is maintained in a designated record set of a covered entity.[131] A covered entity must act on requests for access within 30 days of receiving the request,[132] but may take up to 60 days to act if the requested information is not maintained or accessible to the covered entity on-site.[133] If the covered entity is unable to act within either of these time periods (as applicable), it may take a one-time 30 day extension.[134] Covered entities must provide access to the information in the form or format that the individual requests, if such form or format is readily available. If	The Proposed Rule makes several modifications to this section, applicable when the requested information is maintained electronically in one or more designated record sets, and the individual requests an electronic copy. In such case, covered entities must provide individuals with access to their protected health information in the electronic form and format requested by the individual. If the covered entity cannot produce the information in the requested form or format, it must provide the information in a readable electronic form or format agreed to by the covered entity and the individual. The Proposed Rule expanded the provision requiring covered entities to mail information at the individual's request. Under the Proposed Rule, a covered entity must transmit a copy of protected health information to another	The Final Rule adopts the proposed modifications to this section.[139] The Final Rule modifies the timeliness provisions by removing the provision granting a covered entity 60 days to act when the requested information is not maintained or accessible on-site. Covered entities now have 30 days to act on a request, and may still take a one-time 30 day extension as provided in the original rule.[140]

[130] 78 Fed. Reg. at 5628; 45 C.F.R. § 164.522(a).
[128] 45 C.F.R. §164.522(a)(2)(iii) (2007).
[129] 75 Fed. Reg. at 40899-901.
[131] 45 C.F.R. § 164.524(a)(1) (2007).
[132] 45 C.F.R. § 164.524(b)(2)(i) (2007).
[133] 45 C.F.R. § 164.524(b)(2)(ii) (2007).
[134] 45 C.F.R. § 164.524(b)(2)(iii) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	the requested form or format is not readily available, it must provide a readable hard copy or another form or format agreed to by the covered entity and the individual.[135] The covered entity must mail a copy of the individual's protected health information at the individual's request.[136] The covered entity may charge a reasonable, cost-based fee for providing copies of information (or a summary or explanation of the information, if the individual agrees), which may only include the cost of: (i) copying, including the cost of supplies and labor; (ii) postage, as applicable; and (iii) preparing an explanation or summary of the protected health information, if agreed to by the individual.[137]	person designated by the individual, at the individual's request. Such request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information. The Proposed Rule also modified the provision governing fees a covered entity may charge. The reasonable, cost-based fee may only include the cost of: (i) labor for copying the requested information, whether in paper or electronic form; (ii) supplies for creating the paper copy or electronic media (if the individual requests that the electronic copy be provided on portable media); (iii) postage; and (iv) preparing an explanation or summary.[138]	
§ 164.530 – Administrative requirements	A covered entity must implement policies and procedures to comply with the Privacy Rule,[141] and must	The Interim Final Breach Notification Rule applied the breach notification provisions of subpart D to the	Retains without modification.[150]

[139] 78 Fed. Reg. at 5701; 45 C.F.R. § 164.524(c).
[140] 78 Fed. Reg. ; 45 C.F.R. § 164.524(b)(2)(ii).
[135] 45 C.F.R. § 164.524(c)(2)(i) (2007).
[136] 45 C.F.R. § 164.524(c)(3) (2007).
[137] 45 C.F.R. § 164.524(c)(4) (2007).
[138] 75 Fed. Reg. at 40923-24.
[141] 45 C.F.R. § 164.530(i)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	accordingly train its workforce.[142] It must change such policies and procedures to comply with changes in the law, including changes to the Privacy Rule,[143] and must re-train each member of its workforce whose functions are affected by a material change.[144] A covered entity must provide a complaint process for individuals concerning its compliance with the Privacy Rule,[145] and apply sanctions against its workforce members for noncompliance.[146] A covered entity is prohibited from engaging in intimidating or retaliatory acts against an individual for exercising a right, or for participating in any process, provided for by the Privacy Rule,[147] and from requiring an individual to waive his or her rights under the Privacy Rule as a condition of treatment, payment, enrollment, or eligibility.[148]	administrative requirements. Covered entities must comply with these requirements in addition to the requirements of the Privacy Rule where specified.[149] The Interim Final Breach Notification Rule also added that a covered entity is required to maintain documentation sufficient to meets its burden of proof under § 164.414(b).	

[150] 78 Fed. Reg. at 5566; 45 C.F.R. § 164.530.
[142] 45 C.F.R. § 164.530(b)(1) (2007).
[143] 45 C.F.R. § 164.530(i)(2)(i) (2007).
[144] 45 C.F.R. § 164.530(b)(2)(i)(C) (2007).
[145] 45 C.F.R. § 164.530(d)(1) (2007).
[146] 45 C.F.R. § 164.530(e)(1) (2007).
[147] 45 C.F.R. § 164.530(g)(1) (2007).
[148] 45 C.F.R. § 164.530(h) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.532 – Transition provisions	This section established transition rules for prior authorizations and prior business associate contracts or other arrangements to ensure that covered entities have sufficient time to become compliant with the new HIPAA rules. A covered entity (other than a small health plan) may have a written contract or other arrangement with a business associate that does not comply with §§ 164.502(e) and 164.504(e), if the covered entity is "deemed compliant."[151] A covered entity is "deemed compliant" if it meets certain qualifications, including that it entered into the contract or other arrangement prior to the date the Final Rule is published, and that it does not renew or modify the contract or other arrangement during the set transition period.[152] A prior contract or other arrangement that meets these requirements will only be "deemed compliant" for a limited time period.[153] Another provision permits a covered entity to use or disclose protected	The Proposed Rule modified the provisions governing prior contracts or other arrangements with business associates. Under the Proposed Rule, a covered entity (including a small health plan), or a business associate with respect to a subcontractor, may have a contract or other arrangement that does not comply with §§ 164.308(b), 164.314(a), 164.502(e) and 164.504(e) if the covered entity or business associate is "deemed compliant." The Proposed Rule retains the qualifications for "deemed compliance" of a covered entity and applies them to business associates with respect to subcontractors. The Proposed Rule adds that the contract or other arrangement entered into prior to the publication date of the Final Rule must comply with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date.[155]	The Final Rule adopts the proposed modifications to the provisions governing prior contracts or other arrangements, inserts specific dates as necessary and makes additional modifications.[156] "Deemed compliance" occurs where the covered entity or business associate enters into the contract or other arrangement prior to January 25, 2013, which then cannot be renewed or modified from March 26, 2013 until September 23, 2013. The deemed compliance period ends on the date the contract or other arrangement is renewed or modified (which may not occur before September 23, 2013), but in no case later than September 22, 2014. The Final Rule modifies the provision permitting a covered entity to use or disclose information for research by adding "a waiver of authorization in accordance with § 164.512(i)(1)(i)" to the list of items sufficient to meet this standard, provided that the covered entity satisfies all other requirements.

[149] 74 Fed. Reg. at 42769.
[151] 45 C.F.R. § 164.532(d) (2007).
[152] 45 C.F.R. § 164.532(e)(1) (2007).
[153] 45 C.F.R. § 164.532(e)(2) (2007).
[155] 75 Fed. Reg. at 40889-90.
[156] 78 Fed. Reg. at 5603; 45 C.F.R. § 164.532.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	information that it created or received for research, without obtaining an authorization that meets the requirements of §§ 164.508 or 164.512(i). There may not be an agreed-to restriction on the use or disclosure (in accordance with § 164.522(a)), and the covered entity must obtain one of the following items prior to the applicable compliance date: an authorization (or other express legal permission) from the individual, the individual's informed consent to participate in the research, or a waiver of informed consent by an IRB.[154]		The Final Rule adds a provision applicable to a covered entity that entered into a data use agreement with a recipient of a limited data set prior to January 25, 2013. If the agreement complies with § 164.514(e), the covered entity may continue to disclose the limited data set in exchange for remuneration until the date the agreement is renewed or modified (which cannot be before September 23, 2013), and in no case later than September 22, 2014.[157]
§ 164.302 – Applicability	Covered entities must comply with the requirements of the Security Rule with respect to electronic protected health information.[158]	The Proposed Rule applied this section to business associates.[159]	Adopts as proposed.[160]
§ 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	The Proposed Rule inserted reference to business associates in the definitions of *administrative safeguards* and *physical safeguards*.[164] The Interim Final Breach Notification Rule amended the definition of *access* to note that the definition also does not	Adopts as proposed.[166]

[154] 45 C.F.R. § 164.532(c) (2007).
[157] 78 Fed. Reg. at ; 45 C.F.R. § 164.532(f).
[158] 45 C.F.R. § 164.302 (2007).
[159] 75 Fed. Reg. at 40882.
[160] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.106.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	relation to the protection of that information.[161] *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.[162] *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.[163]	apply to "access" as used within the Breach Notification Rule.[165]	
§ 164.306 – Security standards: General rules	Generally, a covered entity must: (1) ensure the confidentiality, integrity, and 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	The Proposed Rule applied the general requirements for security standards to business associates in the same manner as they apply to covered entities.[176]	Adopts as proposed.[177]

[164] 75 Fed. Reg. at 40882.
[166] 78 Fed. Reg. at 5693; 45 C.F.R. § 164.304.
[161] 45 C.F.R. § 164.304, at "Administrative safeguards" (2007).
[162] 45 C.F.R. § 164.304, at "Physical safeguards" (2007).
[163] 45 C.F.R. § 164.304, at "Access" (2007).
[165] 74 Fed. Reg. at 42756.
[176] 75 Fed. Reg. at 40882.
[177] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.306.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	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.[167] Covered entities must comply with the standards provided in the Security Rule with respect to all electronic protected health information.[168] Most standards identified in the Security Rule include implementation specifications. Implementation specifications are either "required" or "addressable."[169] Covered entities must implement all "required" implementation specifications as written.[170] If an implementation specification is "addressable," the covered entity must assess whether, in the covered entity's environment, the specification would reasonably and appropriately safeguard the covered entity's electronic protected health information.[171] If it would, the covered entity must implement the		

[167] 45 C.F.R. § 164.306(a) (2007).
[168] 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).
[169] 45 C.F.R. § 164.306(d)(1) (2007).
[170] 45 C.F.R. § 164.306(d)(2) (2007).
[171] 45 C.F.R. § 164.306(d)(3)(i) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	specification. If it would not, the covered entity must document why, and, if reasonable and appropriate, adopt an equivalent alternative measure.[172] A covered entity may use any security measures to satisfy the Security Rule's standards and implementation specifications.[173] When deciding what measures to use, the covered entity must take four specific factors into account.[174] The covered entity must review the security measures it uses and modify them as needed.[175]		
§ 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 procedures to prevent, detect, contain and correct security violations.[178] There are four required implementation specifications: (i) conduct a risk	The Proposed Rule applied this section to business associates in the same manner as it applies to covered entities.[198] The Proposed Rule makes a technical change to the third standard's specification requiring implementation of access termination procedures, such that the procedures for terminating access apply when the workforce	Adopts as proposed.[201]

[172] 45 C.F.R. § 164.306(d)(3)(ii) (2007).
[173] 45 C.F.R. § 164.306(b)(1) (2007).
[174] 45 C.F.R. § 164.306(b)(2) (2007).
[175] 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).
[178] 45 C.F.R. § 164.308(a)(1)(i) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	analysis; (ii) implement risk management measures; (iii) enforce a sanction policy; and (iv) implement procedures to review information system activity records.[179] The second standard requires covered entities to assign responsibility for the development and implementation of the policies and procedures required by the Security Rule.[180] The third standard requires covered entities to implement workforce security policies and procedures to ensure appropriate access to electronic protected health information.[181] 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.[182] The fourth standard requires covered entities to implement policies and procedures for information access management that are consistent with	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*.[199] 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.[200] It removed the provision holding a business associate that is also a covered entity responsible for its violation of 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.	

[198] 75 Fed. Reg. at 40882.
[201] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.308.
[179] 45 C.F.R. § 164.308(a)(1)(ii) (2007).
[180] 45 C.F.R. § 164.308(a)(2) (2007).
[181] 45 C.F.R. § 164.308(a)(3)(i) (2007).
[182] 45 C.F.R. § 164.308(a)(3)(ii) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	the applicable requirements of the Privacy Rule.[183] There is one required implementation specification: isolate health care clearinghouse functions from unauthorized access,[184] and two addressable implementation specifications: (i) implement policies and procedures for access authorization,[185] and (ii) implement policies and procedures to establish and modify access.[186] The fifth standard requires covered entities to implement a security awareness and training program for all members of its workforce.[187] There are four addressable implementation specifications: (i) implement periodic security updates; (ii) implement procedures to protect against malicious software; (iii) implement procedures to monitor log-ins; and (iv) implement procedures for password management.[188] The sixth standard requires covered		

[199] 75 Fed. Reg. at 40882.
[200] 75 Fed. Reg. at 40883.
[183] 45 C.F.R. § 164.308(a)(4)(i) (2007).
[184] 45 C.F.R. § 164.308(a)(4)(ii)(A) (2007).
[185] 45 C.F.R. § 164.308(a)(4)(ii)(B) (2007).
[186] 45 C.F.R. § 164.308(a)(4)(ii)(C) (2007).
[187] 45 C.F.R. § 164.308(a)(5)(i) (2007).
[188] 45 C.F.R. § 164.308(a)(5)(ii) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	entities to implement policies and procedures to address security incidents.[189] There is one required implementation specification: implement security incident response and reporting.[190] The seventh standard requires covered entities to establish and implement as needed a contingency plan.[191] 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.[192] The eighth standard requires covered entities to perform a periodic technical and nontechnical evaluation to establish the extent to which an entity's security policies and procedures meet		

[189] 45 C.F.R. § 164.308(a)(6)(i) (2007).
[190] 45 C.F.R. § 164.308(a)(6)(ii) (2007).
[191] 45 C.F.R. § 164.308(a)(7)(i) (2007).
[192] 45 C.F.R. §164.308(a)(7)(ii) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	the requirements of the Security Rule.[193] 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.[194] 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).[195] 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.[196] This standard is not applicable to covered entities in certain situations that do not give rise to a business associate relationship.[197]		

[193] 45 C.F.R. § 164.308(a)(8) (2007).
[194] 45 C.F.R. § 164.308(b)(1) (2007).
[195] 45 C.F.R. § 164.308(b)(4) (2007) (referencing applicable requirements in § 164.314(a)).
[196] 45 C.F.R. §164.308(b)(3) (2007).
[197] 45 C.F.R. § 164.308(b)(2) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 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.[202] 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.[203] The second standard requires covered entities to implement workstation use policies and procedures.[204] The third standard requires covered entities to implement physical safeguards for all workstations that access electronic protected health information.[205] The fourth standard requires covered	The Proposed Rule applied this section to business associates in the same manner that it applies to covered entities.[208]	Adopts as proposed.[209]

[202] 45 C.F.R. § 164.310(a)(1) (2007).
[203] 45 C.F.R. § 164.310(a)(2) (2007).
[204] 45 C.F.R. §164.310(b) (2007).
[205] 45 C.F.R. § 164.310(c) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	entities to implement device and media control policies and procedures.[206] 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.[207]		
§ 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.[210] 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; and (ii) implement a mechanism to encrypt and decrypt	The Proposed Rule applied this section to business associates in the same manner as it applies to covered entities.[218]	Adopts as proposed.[219]

[208] 75 Fed. Reg. at 40882.
[209] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.310.
[206] 45 C.F.R. § 164.310(d)(1) (2007).
[207] 45 C.F.R. § 164.310(d)(2) (2007).
[210] 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
	electronic protected health information.[211] The second standard requires covered entities to implement audit controls.[212] The third standard requires covered entities to implement policies and procedures to protect the integrity of electronic protected health information.[213] There is one addressable implementation specification: implement mechanisms to authenticate electronic protected health information.[214] 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.[215] The fifth standard requires covered entities to implement technical transmission security measures.[216] There are two addressable		

[218] 75 Fed. Reg. at 40882.
[219] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.312.
[211] 45 C.F.R. § 164.312(a)(2) (2007).
[212] 45 C.F.R. § 164.312(b) (2007).
[213] 45 C.F.R. § 164.312(c)(1) (2007).
[214] 45 C.F.R. § 164.312(c)(2) (2007).
[215] 45 C.F.R. § 164.312(d) (2007).
[216] 45 C.F.R. § 164.312(e)(1) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	implementation specifications: (i) implement integrity controls; and (ii) implement an encryption mechanism.[217]		
§ 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[220] satisfy the applicable implementation specification.[221] 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).[222]	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.[226] 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.[227] 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.[228]

[217] 45 C.F.R. § 164.312(e)(2) (2007).
[220] 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).
[221] 45 C.F.R. § 164.314(a)(1)(i) (2007).
[222] 45 C.F.R. § 164.314(a)(1)(ii) (2007).
[226] 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.[223] The implementation specification for "other arrangements" set forth requirements applicable to three specific types of arrangements.[224] The second standard sets forth requirements applicable to a group health plan.[225]	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.[233]

[227] 75 Fed. Reg. at 40883.
[228] 78 Fed. Reg. at 5591; 45 C.F.R. § 164.314.
[223] 45 C.F.R. § 164.314(a)(2)(i) (2007).
[224] 45 C.F.R. § 164.314(a)(2)(ii) (2007).
[225] 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.[229] 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.[230] 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.[231]	entities.[232]	
§ 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.[234]	Retains without modification.[235]
	The HIPAA rules reserved subpart D	The Interim Final Breach Notification	The Final Rule modifies the definition

[233] 78 Fed. Reg. at 5695; 45 C.F.R. § 164.316.
[229] 45 C.F.R. § 164.316(a) (2007).
[230] 45 C.F.R. § 164.316(b)(1) (2007) (Note that "written form" may be electronic).
[231] 45 C.F.R. § 164.316(b)(2) (2007).
[232] 75 Fed. Reg. at 40882.
[234] 74 Fed. Reg. at 42743.
[235] 78 Fed. Reg. at 5566; 45 C.F.R. § 164.400.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.402 – Definitions, *breach*	for future use, but do not include any content therein.	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),[236] 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 permitted under the Privacy Rule; (ii) any inadvertent disclosure by a person	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.[238] The Final Rule retains all three exclusions from the definition of breach without modification.[239]

[236] 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)).
[238] 78 Fed. Reg. at 5641; 45 C.F.R. § 164.402, at ¶ (2) of "Breach."
[239] 78 Fed. Reg. at 5695; 45 C.F.R. § 164.402, at ¶ (1) of "Breach."

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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.[237]	
§ 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.[240]	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.[241]
§ 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, to notify each individual	Retains without modification.[243]

[237] 74 Fed. Reg. at 42743.
[240] 74 Fed. Reg. at 42743.
[241] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.402.
[243] 78 Fed. Reg. at 5647, 49; 45 C.F.R. § 164.404.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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.[242]	

[242] 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 content therein.	The Interim Final Breach Notification Rule required covered entities, following discovery of a breach	The Final Rule retains this section, but removes the reference to American Samoa and Northern Mariana Islands,

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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.[244]	which are now included in the definition of *State* in § 160.103.[245]
§ 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.[246]	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.[247]
§ 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 discovery of a breach of unsecured	Retains without substantive modification.[249]

[244] 74 Fed. Reg. at 42752.
[245] 78 Fed. Reg. at 5653; 45 C.F.R. § 164.406.
[246] 74 Fed. Reg. at 42753.
[247] 78 Fed. Reg. at 5654; 45 C.F.R. § 164.408.
[249] 78 Fed. Reg. at 5656; 45 C.F.R. § 164.410.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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).[248]	
§ 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 orally, the covered entity or business	Retains without modification.[251]

[248] 74 Fed. Reg. at 42753.
[251] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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.[250]	
§ 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.[252]	Retains without modification.[253]
§ 160.300 – Applicability	The provisions of the Enforcement Rule governing compliance and investigations apply to covered entities.[254]	The Proposed Rule added that these provisions apply to business associates.[255]	Adopts as proposed.[256]
§ 160.304 – Principles for achieving	To the extent practicable, the Secretary will seek the cooperation of covered	The Proposed Rule added that the Secretary will seek cooperation	Adopts as proposed.[260]

[250] 74 Fed. Reg. at 42755.
[252] 74 Fed. Reg. at 42755.
[253] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.414.
[254] 45 C.F.R. § 160.300 (2007).
[255] 75 Fed. Reg. at 40875.
[256] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.300.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
compliance	entities in obtaining compliance with the applicable HIPAA provisions.[257] The Secretary may provide technical assistance to covered entities to help them comply voluntarily.[258]	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.[259]	
§ 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,[261] who may choose to investigate such complaints.[262]	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.[263]	Adopts as proposed.[264]
§ 160.308 – Compliance reviews	The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable HIPAA provisions.[265]	The Proposed Rule applied this provision to business associates. The 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	Adopts as proposed.[267]

[260] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.304.
[257] 45 C.F.R. § 160.304(a) (2007).
[258] 45 C.F.R. § 160.304(b) (2007).
[259] 75 Fed. Reg. at 40875-76.
[261] 45 C.F.R. § 160.306(a) (2007).
[262] 45 C.F.R. § 160.306(c) (2007).
[263] 75 Fed. Reg. at 40876.
[264] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.306.
[265] 45 C.F.R. § 160.308 (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		compliance reviews in any other circumstances.[266]	
§ 160.310 – Responsibilities of covered entities	Covered entities must keep records and submit compliance reports in accordance with the Secretary's requirements.[268] Covered entities must cooperate with the Secretary during an investigation or compliance review,[269] 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.[270] 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 efforts it has made to obtain the information.[271] The Secretary may only disclose the protected health information she obtains in connection with an investigation or compliance review as	The Proposed Rule applied the requirements of this section to business associates, and re-titled the section "Responsibilities of covered entities and business associates."[273] 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.[274]	Adopts as proposed.[275]

[267] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.308.
[266] 75 Fed. Reg. at 40876.
[268] 45 C.F.R. § 160.310(a) (2007).
[269] 45 C.F.R. § 160.310(b) (2007).
[270] 45 C.F.R. § 160.310(c)(1) (2007).
[271] 45 C.F.R. § 160.310(c)(2) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	is necessary to ascertain or enforce compliance, or as otherwise required by law.[272]		
§ 160.312 – Secretarial action regarding complaints and compliance reviews	The Secretary must try to informally resolve matters of noncompliance.[276] 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.[277] The Secretary will inform the covered entity in a notice of proposed determination if she finds that a civil monetary penalty should be imposed.[278]	The Proposed Rule applied this section to business associates and gave the Secretary discretion to informally resolve matters of noncompliance.[279]	Adopts as proposed.[280]
§ 160.316 – Refraining from intimidation or retaliation	Covered entities may not take any 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	The Proposed Rule applied this section to business associates.[282]	Adopts as proposed.[283]

[273] 75 Fed. Reg. at 40876.
[274] 75 Fed. Reg. at 40876.
[275] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.310.
[272] 45 C.F.R. § 160.310(c)(3) (2007).
[276] 45 C.F.R. § 160.312(a)(1) (2007).
[277] 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).
[278] 45 C.F.R. § 160.312(a)(3)(ii) (2007) (referencing § 160.420, governing notices of proposed determinations).
[279] 75 Fed. Reg. at 40876-77.
[280] 78 Fed. Reg. at 5578; 45 C.F.R. § 160.312.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	and without violating the Privacy Rule.[281]		
§ 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.[284] *Reasonable diligence* is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.[285] *Willful neglect* is the conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA provision that was violated.[286]	The Interim Final Enforcement Rule added § 160.401 and included the terms *reasonable cause*, *reasonable diligence*, and *willful neglect*, as defined in § 160.410.[287] 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.[288]	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*.[289]
§ 160.402 –	The Secretary will impose a civil	The Proposed Rule applied the	Adopts as proposed.[295]

[282] 75 Fed. Reg. at 40875.
[283] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.316.
[281] 45 C.F.R. § 160.316 (2007).
[284] 45 C.F.R. § 160.410(a), at "Reasonable cause" (2007).
[285] 45 C.F.R. § 160.410(a), at "Reasonable diligence" (2007).
[286] 45 C.F.R. § 160.410(a), at "Willful neglect" (2007).
[287] HIPAA Administrative Simplification: Enforcement; Interim Final Rule with Request for Comments, 74 Fed. Reg. 56123, at 56126 (October 30, 2009).
[288] 75 Fed. Reg. at 40877.
[289] 78 Fed. Reg. at 5580; 45 C.F.R. § 160.401.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
Basis for a civil money penalty	monetary penalty on a covered entity for violating a HIPAA provision.[290] If more than one covered entity was responsible for a violation, the Secretary will impose a civil monetary penalty on each responsible covered entity.[291] 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.[292] 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.[293]	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.[294] 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.	
§ 160.404 – Amount of a civil money penalty	The Secretary may not impose a civil monetary penalty that exceeds $100 per violation,[296] or that exceeds $25,000 for	The Interim Final Enforcement Rule modified this section so that the existing limits on the imposition of	The Final Rule made no additional changes to the Interim Final Rule's modifications,[301] and accepted the

[295] 78 Fed. Reg. at 5581; 45 C.F.R. § 160.402.
[290] 45 C.F.R. § 160.402(a) (2007).
[291] 45 C.F.R. § 160.402(b)(1) (2007).
[292] 45 C.F.R. § 160.402(b)(2) (2007).
[293] 45 C.F.R. § 160.402(c) (2007).
[294] 75 Fed. Reg. at 40879.
[296] 45 C.F.R. § 160.404(b)(1)(i) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	identical violations during a calendar year.[297]	civil monetary penalties apply only to violations occurring before February 18, 2009.[298] 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.[299] 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.[300]	penalty tier structure as modified by the Proposed Rule.[302]
§ 160.406 – Violations of an identical requirement or prohibition	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 act under the provision that is violated.[303] A separate violation occurs	The Proposed Rule applied this section to business associates.[304]	Adopts as proposed.[305]

[301] 78 Fed. Reg. at 5577, 5583; 45 C.F.R. § 160.404.
[297] 45 C.F.R. § 160.404(b)(1)(ii) (2007).
[298] 74 Fed. Reg. at 56126
[299] 74 Fed. Reg. at 56126
[300] 75 Fed. Reg. at 40875.
[302] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.404.
[303] 45 C.F.R. § 160.406 (2007).
[304] 75 Fed. Reg. at 40875.
[305] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.406.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	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.[306]	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.[307]	Adopts as proposed.[308]
§ 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[309]; (2) the covered entity lacked knowledge of the violation and would not have known that the violation occurred by	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 neglect, and is corrected within the prescribed time period.[311]	The Final Rule adopts the Proposed Rule's modifications.[313]

[306] 45 C.F.R. § 164.408 (2007).
[307] 75 Fed. Reg. at 40880-81.
[308] 78 Fed. Reg. at 5577, 5585; 45 C.F.R. § 160.408.
[309] Social Security Act § 1177, 42 U.S.C. § 1320d-6.
[311] 74 Fed. Reg. at 56128 – 29.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	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.[310]	The Proposed Rule made additional revisions to this section.[312] 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 after February 18, 2009, the Proposed Rule adopted the Interim Final Rule's modified third defense and expanded it	

[313] 78 Fed. Reg. at 5577, 5586; 45 C.F.R. § 160.410.
[310] 45 C.F.R. § 160.410(b) (2007).
[312] 75 Fed. Reg. at 40881.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		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.[314]	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.[315]	Adopts as proposed.[316]
§ 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.[317] This notice must include, among other things, the amount of the proposed penalty.[318]	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.[319]	Retains without modification.[320]
§ 160.534 – The hearing	In a hearing with an ALJ, the respondent has the burden of persuasion with respect to any: (i) affirmative defense;[321] (ii) challenge to the amount of the proposed penalty, including any mitigating factors;[322] or (iii) claim that a proposed penalty should be reduced or waived.[323] The	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 breach). The Interim Final Rule further noted that the Secretary has the burden	Retains without modification.[326]

[314] 45 C.F.R. § 160.418 (2007) (referencing 42 U.S.C. § 1320d-5(b)(1)).
[315] 75 Fed. Reg. at 40881.
[316] 78 Fed. Reg. at 5586; 45 C.F.R. § 160.418.
[317] 45 C.F.R. § 160.420(a) (2007).
[318] 45 C.F.R. § 160.420(b) (referencing § 160.504, governing ALJ hearing requests).
[319] 74 Fed. Reg. 56129.
[320] 78 Fed. Reg. at 5586; 45 C.F.R. § 160.420(a)(4).
[321] 45 C.F.R. § 160.534(b)(1)(i) (2007) (referencing § 160.410, governing affirmative defenses).
[322] 45 C.F.R. § 160.534(b)(1)(ii) (2007) (referencing §§ 160.404 – 160.408, governing penalties).
[323] 45 C.F.R. § 160.534(b)(1)(iii) (2007) (referencing § 160.412, governing reductions/waivers of proposed penalties).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	Secretary has the burden of persuasion with respect to all other issues, including issues of liability and the existence of any aggravating factors.[324]	of persuasion with respect to all other issues except for issues of liability under the Breach Notification Rule.[325]	
§ 160.101 – Statutory basis and purpose	The requirements in the HIPAA regulations are based on the regulations in §§ 1171 – 1179 of the Social Security Act (as added by HIPAA § 262), and on § 264 of HIPAA.[327]	The Proposed Rule added a reference to §§ 13400 – 13424 of HITECH,[328] and the Proposed GINA Rule added references to § 105 of GINA and § 1180 of the Social Security Act[329] as bases for the proposed requirements.	Adopts as proposed.[330]
§ 160.102 – Applicability	The HIPAA rules apply to *covered entities*, 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.[331]	The Proposed Rule added a provision stating that the HIPAA rules apply to business associates where specified.[332]	Adopts as proposed.[333]
§ 160.103 – Definitions, *business*	A *business associate* is a person who, on behalf of a covered entity (or on	The Proposed Rule added "patient safety activities" to the list of activities	Adopts as proposed.[340]

[326] 78 Fed. Reg. at 5569; 45 C.F.R. § 160.534(b).
[324] 45 C.F.R. § 160.534(b)(2) (2007).
[325] Breach Notification for Unsecured Protected Health Information; Interim Final Rule with Request for Comments, 74 Fed. Reg. 42740, at 42755 (August 24, 2009).
[327] 45 C.F.R. § 160.101 (2007) (Note that the July 2011 IFR proposing operating rules for eligibility for a health plan and health care claims status added a reference to § 1104 of the Affordable Care Act, which was included in 45 C.F.R. § 160.101 as of 2011).
[328] Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Notice of Proposed Rulemaking, 75 Fed. Reg. 40868, 40872 (July 14, 2010) (Note that the Breach Notification IFR added a reference to HITECH Act § 13402, which was included in the CFR as of 2009, and the Enforcement IFR added a reference to HITECH Act § 13410(d), which was included in the CFR as of 2010).
[329] HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information; Notice of Proposed Rulemaking, 74 Fed Reg. 51698, 51708 (October 7, 2009).
[330] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule 78 Fed. Reg. 5566, 5570 and 5661 (January 25, 2013) (to be codified at 45 C.F.R. § 160.101).
[331] 45 C.F.R. § 160.102(a) (2007).
[332] 75 Fed. Reg. at 40872.
[333] 78 Fed. Reg. at 5570; 45 C.F.R. § 160.102(b).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
associate	behalf of an organized health care arrangement in which the covered entity participates), performs or helps perform any function or activity that involves the use or disclosure of individually identifiable health information, or that is otherwise regulated by the HIPAA rules.[334] A person who provides certain services to or for a covered entity (or to or for an organized health care arrangement in which the covered entity participates) is a *business associate* when provision of the service involves the disclosure of individually identifiable health information from the covered entity or arrangement to the person.[335] A member of the covered entity or organized health care arrangement's workforce is not considered a business associate in either situation.	that create a business associate relationship when performed on behalf of a covered entity or arrangement.[336] The Proposed Rule changed the term "individually identifiable health information" to "protected health information."[337] The Proposed Rule specifically identified three types of entities as *business associates*: (i) Health Information Organizations, E-prescribing Gateways, or other persons that provide data transmission services of protected health information to a covered entity and who require access on a routine basis to such information; (ii) a person that offers personal health records to individuals on behalf of a covered entity; and (iii) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate.[338] The Proposed Rule moved provisions from §§ 164.308 and 164.502 excluding certain recipients of	The Final Rule further modifies *business associate* such that a business associate is a person who, on behalf of a covered entity (or on behalf of an organized health care arrangement in which the covered entity participates), creates, receives, maintains, or transmits protected health information for a function or activity that is regulated by the HIPAA rules.[341]

[340] 78 Fed. Reg. at 5571-73; 45 C.F.R. § 160.103, at "Business associate."
[334] 45 C.F.R. § 160.103, at ¶ (1)(i) of "Business associate" (2007).
[335] 45 C.F.R. § 160.103, at ¶ (1)(ii) of "Business associate" (2007).
[336] 75 Fed. Reg. at 40872.
[337] 75 Fed. Reg. at 40874.
[338] 75 Fed. Reg. at 40872-74.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		protected health information to the definition of *business associate*.[339]	
§ 160.103 – Definitions, *subcontractor*	The HIPAA Rules do not define *subcontractor*.	The Proposed Rule defined *subcontractor* as "a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate."[342]	The Final Rule defines *subcontractor* as a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.[343]
§ 160.103 – Definitions, *protected health information*	*Protected health information* is individually identifiable health information that is transmitted or maintained in any form or medium.[344] The definition excludes individually identifiable health information in certain education records and in employment records held by a covered entity in its role as employer.[345]	The Proposed Rule also excluded individually identifiable health information regarding persons who have been deceased for over 50 years from *protected health information*.[346]	Adopts as proposed.[347]
§ 160.103 – Definitions, *State*	*State* includes any of the several States, D.C., Puerto Rico, the Virgin Islands, and Guam.[348]	The Proposed Rule included American Samoa and the Northern Mariana Islands in *State*.[349]	Adopts as proposed.[350]
§ 160.103 – Definitions, *electronic*	*Electronic media* is electronic storage media[351] or transmission media used to	The Proposed Rule replaced "electronic storage media" with	Adopts as proposed.[354]

[341] 78 Fed. Reg. at 5572, 74; 45 C.F.R. § 160.103, at ¶ (1)(i) of "Business Associate."
[339] 75 Fed. Reg. at 40873 – 74 (referencing the provisions at § 164.308(b)(2) and § 164.502(e)(1)(ii)).
[342] 75 Fed. Reg. at 40873.
[343] 78 Fed. Reg. at 5689; 45 C.F.R. § 160.103, at "Subcontractor."
[344] 45 C.F.R. § 160.103, at ¶ (1) of "Protected health information" (2007).
[345] 45 C.F.R. § 160.103, at ¶ (2) of "Protected health information" (2007).
[346] 75 Fed. Reg. at 40874.
[347] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103, at ¶ (2)(iv) of "Protected health information."
[348] 45 C.F.R. § 160.103, at ¶ (2) of "State" (2007).
[349] 75 Fed. Reg. at 40874.
[350] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103, at ¶ (2) of "State."
[351] 45 C.F.R. § 160.103, at ¶ (1) of "Electronic media" (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
media	exchange information already in electronic storage media.[352] Transmission media includes the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/ transportable electronic storage media. Transmissions via electronic media exclude transmissions where the information being exchanged did not exist in electronic form before the transmission.	"electronic storage material on which data is or may be recorded electronically."[353] The Proposed Rule expanded the list of examples of transmission media to include "extranet **or intranet**."	The Final Rule further amends the list of transmission media examples by removing the phrase "wide open" after Internet and removing the language following "extranet or intranet."[355] The Final Rule also clarifies that transmissions via electronic media exclude transmissions only where the information being exchanged did not exist in electronic form **immediately** before the transmission.
§ 160.103 – Definitions, *health information*	*Health information* is any information that is created or received by a specified entity and that relates to an individual's health or condition, provision of health care to an individual, or payment for such care.[356]	The Proposed GINA Rule amended the definition so that *health information* expressly includes genetic information.[357]	Adopts as proposed.[358]
§ 160.103 – Definitions, *genetic*	The HIPAA rules do not define *genetic information*.	The Proposed GINA Rule defined *genetic information* as information about: (i) an individual's genetic tests;	Adopts as proposed.[360]

[354] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103, at "Electronic media."
[352] 45 C.F.R. § 160.103, at ¶ (2) of "Electronic media" (2007).
[353] 75 Fed. Reg. at 40874.
[355] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103, at ¶ (2) of "Electronic media."

[356] 45 C.F.R. § 160.103, at "Health information" (2007).
[357] 74 Fed Reg. at 51700.
[358] 78 Fed. Reg. at 5661; 45 C.F.R. § 160.103.
[360] 78 Fed. Reg. at 5662; 45 C.F.R. § 160.103, at "Genetic information."

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
information		(ii) an individual's family members' genetic tests; (iii) the manifestation of a disease or disorder in an individual's family member; or (iv) an individual or his or her family member's request for or receipt of genetic services, or participation in clinical research that includes genetic services. Genetic information about an individual or his or her family member includes the genetic information of a fetus carried, or an embryo held using assisted reproductive technology, by the individual or family member. An individual's age and sex are not genetic information.[359]	
§ 160.103 – Definitions, *genetic test*	The HIPAA rules do not define *genetic test*.	The Proposed GINA Rule defined *genetic test* as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes." This definition does not include an analysis of proteins or metabolites that is directly related to "a manifested disease, disorder, or pathological condition."[361]	Adopts as proposed.[362]
§ 160.103 – Definitions, *genetic services*	The HIPAA rules do not define *genetic services*.	The Proposed GINA Rule defined *genetic services* as: (1) a genetic test;	Adopts as proposed.[364]

[359] 74 Fed. Reg. at 51700.
[361] 74 Fed. Reg. at 51700-01.
[362] 78 Fed. Reg. at 5662; 45 C.F.R. § 160.103, at "Genetic test."

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
		(2) genetic counseling; or (3) genetic education.[363]	
§ 160.103 – Definitions, *family member*	The HIPAA rules do not define *family member*.	The Proposed GINA Rule defined *family member* as: (1) an individual's dependent; or (2) a first, second, third, or fourth degree relative of the individual or his or her dependent. The rule treats relatives by law (e.g., marriage or adoption), as well as less than full-blood relatives (e.g., half-siblings), in the same manner as full-blood relatives.[365]	Adopts as proposed.[366]
§ 160.103 – Definitions, *manifestation or manifested*	The HIPAA rules do not define *manifestation* or *manifested*.	The Proposed GINA Rule defined *manifestation* or *manifested* with respect to a disease, disorder, or pathological condition to mean that "an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved." A disease, disorder, or pathological condition is not manifested if the diagnosis is primarily based on genetic information.[367]	Adopts as proposed.[368]
§ 160.105 –	The HIPAA rules do not contain §	The Proposed Rule added this section	Adopts as proposed.[370]

[364] 78 Fed. Reg. at 5663; 45 C.F.R. § 160.103.
[363] 74 Fed. Reg. at 51701.
[365] 74 Fed. Reg. at 51701.
[366] 78 Fed. Reg. at 5663; 45 C.F.R. § 160.103, at "Family member."
[367] 74 Fed. Reg. at 51701-02.
[368] 78 Fed. Reg. at 5569; 45 C.F.R. § 160.103, at "Manifestation or manifested".
[370] 78 Fed. Reg. at 5569; 45 C.F.R. § 160.105.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
Compliance dates for implementation of new or modified standards and implementation specifications	160.105.	to give covered entities and business associates 180 days after the effective date of the Final Rule to comply with the new or amended requirements. Any future changes to the HIPAA rules will also be subject to a 180-day compliance period [369]	The effective date of the Final Rule will be March 26, 2013. Covered entities and business associates must be in compliance by September 23, 2013.
§ 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.[371]	The Proposed Rule added HITECH §§ 13400 – 13424 as a basis for the authority to prescribe the requirements in Part 164.[372]	Adopts as proposed.[373]
§ 164.103 – Definitions, *law enforcement official*	The HIPAA provisions do not define *law enforcement official* at § 164.103. At § 164.501, *law enforcement official* 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."[374]	The Interim Final Breach Notification Rule moved the definition of *law enforcement official* from § 164.501 to § 164.103, so that it applies to both the Breach Notification and Privacy Rules.[375]	Retains without modification.[376]

[369] 75 Fed. Reg. at 40871.
[371] 45 C.F.R. § 164.102 (2007).
[372] 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).
[373] 78 Fed. Reg. at 5587; 45 C.F.R. § 164.102.
[374] 45 C.F.R. § 164.501, at "Law enforcement official" (2007).
[375] 74 Fed. Reg. at 42755.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
§ 164.104 – Applicability	The provisions of Part 164 apply to *covered entities*, 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.[377] When a health care clearinghouse creates or receives protected health information as it must comply with the organizational requirements for covered entities in §164.105.[378]	The Proposed Rule applied the provisions of Part 164 to business associates where specified.[379] The Proposed Rule removed the language requiring a health care clearinghouse to comply with § 164.105.	Adopts as proposed.[380]
§ 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.[381] 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.[382] A hybrid covered entity has discretion to include other components to the extent that	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.[389] The Proposed Rule removed the provision that specifically required a covered entity to ensure that business	Adopts as proposed.[391] 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.[392] The Final Rule retains a hybrid covered entity's discretion to include in its

[376] 78 Fed. Reg. at 5566; 45 C.F.R. § 164.103, at "Law enforcement official."
[377] 45 C.F.R. § 164.104(a) (2007).
[378] 45 C.F.R. § 164.104(b) (2007).
[379] 75 Fed. Reg. at 40881.
[380] 78 Fed. Reg. at 5587 -88; 45 C.F.R. § 164.104(b).
[381] 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).
[382] 45 C.F.R. § 164.105(a)(2)(iii)(C) (2007).
[389] 75 Fed. Reg. at 40881.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	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 entities). 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.[383] 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.[384] 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,[385] and it must also implement policies and procedures to ensure compliance with	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.[390] 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. The Proposed Rule combined the safeguarding provisions applicable to affiliated covered entities into one provision.	health care component other components to the extent they perform covered functions.

[391] 78 Fed. Reg. at 5588; 45 C.F.R. § 164.105.
[392] 78 Fed. Reg. at 5588; 45 C.F.R. § 164.105(a)(2)(iii)(D).
[383] 45 C.F.R. § 164.105(a)(2)(ii) (2007).
[384] 45 C.F.R. § 164.105(a)(2)(ii)(C), (D) (2007).
[385] 45 C.F.R. § 164.105(a)(2)(iii)(A) (2007).

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
	this section and the Privacy and Security Rules.[386] Legally affiliated covered entities may designate themselves as a single covered entity for purposes of the Privacy and Security Rules, if all of the designated covered entities are under common ownership or control.[387] 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.[388]		
§ 160.201 – Applicability	The HIPAA regulations governing the preemption of State law implement § 1178 of the Social Security Act, which was added by HIPAA § 262.[393]	The Proposed Rule re-titled this section "Statutory basis" and added references to HIPAA § 264(c) and HITECH § 13421(a).[394]	Adopts as proposed.[395]
§ 160.202 –	When used to compare a provision of	The Proposed Rule expanded the	Adopts as proposed.[399]

[390] 75 Fed. Reg. at 40882.
[386] 45 C.F.R. § 164.105(a)(2)(iii)(B) (2007) (referencing policies and procedures in §§ 164.316(a) and 164.530(i)).
[387] 45 C.F.R. § 164.105(b)(1) (2007) (referencing documentation requirements at § 164.105(c)).
[388] 45 C.F.R. § 164.105(b)(1)(ii) (2007)
[393] 45 C.F.R. § 160.201 (2007). Section 1178 of the Social Security Act (contained within Part C of Title 11, which was added by HIPAA § 262) provides that a HIPAA provision or requirement will supersede any contrary provision of State law unless the State law is more stringent than HIPAA (subject to certain exceptions), or the Secretary determines that the State law is necessary for certain purposes or addresses controlled substances (Social Security Act § 1178, 42 U.S.C. 1320d-7).
[394] 75 Fed. Reg. at 40874-75.
[395] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.201.

Provision	HIPAA Requirements	Proposed/Interim Final Rules	Final Rule
Definitions, *contrary*	State law to a HIPAA provision, *contrary* means that: (1) a covered entity would find it impossible to comply with both provisions;[396] or (2) the State law is an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA's administrative simplification provisions.[397]	definition so that a state law is also *contrary* if a business associate would find it impossible to comply with both provisions, or if the law is an obstacle to the accomplishment and execution of the full purposes and objectives of subtitle D of HITECH (§§ 13400 - 13424).[398]	
§ 160.202 – Definitions, *more stringent*	A State law is *more stringent* than a contrary HIPAA privacy standard (and thus not preempted) if the State law meets one or more of six specified criteria.[400] A State law is not *more stringent* if it prohibits or restricts a disclosure required by the Secretary to determine whether a covered entity is in compliance with the HIPAA regulations.[401]	The Proposed Rule modified *more stringent* so that a state law also does not meet the definition if it prohibits a disclosure required by the Secretary to determine a business associate's compliance.[402]	Adopts as proposed.[403]

[399] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.202.
[396] 45 C.F.R. § 160.202, at ¶ (1) of "Contrary" (2007).
[397] 45 C.F.R. § 160.202, at ¶ (2) of "Contrary" (2007).
[398] 75 Fed. Reg. at 40875.
[400] 45 C.F.R. § 160.202, at "More stringent" (2007).
[401] 45 C.F.R. § 160.202, at ¶ (1)(i) of "More stringent" (2007).
[402] 75 Fed. Reg. at 40875.
[403] 78 Fed. Reg. at 5577; 45 C.F.R. § 160.202, at ¶ (1)(i) of "More stringent."