	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS				
1	The authority citation for part 160 is revised to read as follows: Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d -1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S. C. 1320d-2(note)); 5 U.S.C. 552; secs. 13400 –13424, Pub. L. 111-5, 123 Stat. 258-279 and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.	**Authority:** 42 U.S.C. 1302(a), 42 U.S.C. 1320d 1320d-8, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(*note*)) and 5 U.S.C. 552.	Updated statutory authority for revised regulations.	
2	Revise § 160.101 to read as follows: **§ 160.101 Statutory basis and purpose.** The requirements of this subchapter implement sections 1171 – 1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400 – 13424 of Public Law 111-5, and section 1104 of Public Law 111-148.	**§ 160.101 Statutory basis and purpose.** The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104–191, and section 264 of Public Law 104–191.	Updated statutory basis and purpose for revised regulations.	
3	Amend § 160.102 as follows: a. Redesignate paragraph (b) as paragraph (c); and b. Add new paragraph (b) to read as follows: **§ 160.102 Applicability.** * * * * * (b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate. (c) To the extent required under the Social Security Act, 42 U.S.C. 1320a–7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).	**§ 160.102 Applicability.** (a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (b) To the extent required under the Social Security Act, 42 U.S.C. 1320a–7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).	Inserted a new paragraph (b) to indicate that certain standards, requirements and implementation specifications will apply to business associates (as well as covered entities, which are identified in paragraph (a)).	
4	Amend § 160.103 as follows: a. Revise the definitions of "Business associate", "Compliance date", "Disclosure",		Revised/added definitions necessary to implement the required changes to the privacy and security rules.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	"Electronic media", the introductory text of the definition of "Health Information", paragraphs (1)(vi) through (xi), and (xv) of the definition of "Health Plan", paragraph (2) of the definition of "Protected health information," and the definitions of "Standard", "State", and "Workforce"; and b. Add, in alphabetical order, new definitions of "Administrative simplification provision", "ALJ", "Civil money penalty or penalty", "Family member", "Genetic information", "Genetic services", "Genetic test", "Manifestation or manifested", "Respondent", "Subcontractor", and "Violation or violate". The revisions and additions read as follows: **§ 160.103 Definitions.** * * * * *			
	Administrative simplification provision means any requirement or prohibition established by: (1) 42 U.S.C. 1320d – 1320d–4, 1320d–7, 1320d–8, and 1320d-9; (2) Section 264 of Pub. L. 104–191; (3) Sections 13400 – 13424 of Public L. 111-5; or (4) This subchapter.	*Administrative simplification provision* means any requirement or prohibition established by: (1) 42 U.S.C. 1320d—1320d–4, 1320d–7, and 1320d–8; (2) Section 264 of Pub. L. 104–191; or (3) This subchapter.	Moved this definition from § 160.302 (Compliance and Enforcement) to apply to HIPAA privacy and security rule generally, and added reference to HITECH.	
	ALJ means Administrative Law Judge.	*ALJ* means Administrative Law Judge.	Moved this definition from § 160.302 (Compliance and Enforcement) to apply to HIPAA privacy and security rule generally. No substantive changes to the definition.	
	Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity	*Business associate:* (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of	Modified the definition of business associate to include the activities of Patient Safety Organizations (PSO), as well as Health Information Organizations (this includes RHIOs and HIEs together), e-Prescribing gateway vendors, PHR vendors that offer PHR to individuals on behalf of a covered entity, and subcontractors of business associates that	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity may be a business associate of another covered entity. (3) Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services	such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity.	create receive or maintain PHI on a routine basis. The definition also added certain types of entities that are excluded from the definition of business associates, and revised the wording from reference to "individually identifiable health information" to "protected health information", in order to be more consistent with a definition of business associate under HITECH.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. (4) Business associate does not include: (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual. (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met. (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law. (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as			

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.			
	Civil money penalty or penalty means the amount determined under § 160.404 of this part and includes the plural of these terms.	*Civil money penalty* or *penalty* means the amount determined under §160.404 of this part and includes the plural of these terms.	Moved this definition from § 160.302 (Compliance and Enforcement) to apply to HIPAA privacy and security rule generally. No substantive changes to the definition.	
	Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.	*Compliance date* means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.	Modified the definition to include reference to business associates.	
	Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.	*Disclosure* means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.	Corrected a typographical error to the definition (removed a comma). No substantive change to the definition.	
	Electronic media means: (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and	*Electronic media* means: (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, 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. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form	Prior definition made reference to electronic "media" in paragraph (1). The revision more broadly refers to electronic "material on which data is or may be recorded electronically." Also, clarified that the definition applies to transmission media whether inside or outside an organization's network. In addition, clarified that voice and facsimile transmission are not considered transmission if the information being exchanged did not exist electronically *immediately* before the transmission.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.	before the transmission.		
	Family member means, with respect to an individual: (1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or (2) Any other person who is a first-degree, second-degree, third-degree, or fourth degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents). (i) First-degree relatives include parents, spouses, siblings, and children. (ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces. (iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. (iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.	NEW	Added to implement GINA regulations under HIPAA.	
	Genetic information means:	NEW	Added to implement GINA regulations	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of: (i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex or age of any individual.		under HIPAA.	
	Genetic services means: (1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education.	NEW	Added to implement GINA regulations under HIPAA.	
	Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested	NEW	Added to implement GINA regulations under HIPAA.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	disease, disorder, or pathological condition.			
	Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: * * *	*Health information* means any information, whether oral or recorded in any form or medium, that: * * *	Modified the definition of Health information to include genetic information to implement GINA.	
	Health plan means * * * (1) * * * (vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152. (vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)). (viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy. (ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. (x) The health care program for uniformed services under title 10 of the United States Code. (xi) The veterans health care program under 38 U.S.C. chapter 17. * * * * * (xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.	*Health plan* means * * * (1) * * * (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)). (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy. (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. (ix) The health care program for active military personnel under title 10 of the United States Code. (x) The veterans health care program under 38 U.S.C. chapter 17. (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)). * * * * * (xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.	Modified the definition of Health plan to include Voluntary Prescription Drug Programs under Medicare Part D and the Medicare Advantage program.	
	Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care	NEW	Added to implement GINA regulations under HIPAA.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.			
	Protected health information * * * (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.	*Protected health information* means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.	Modified the definition of PHI to add an exclusion for information relating to a person who has been deceased for more than 50 years.	
	Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.	*Respondent* means a covered entity upon which the Secretary has imposed, or proposes to impose, a civil money penalty.	Moved this definition from § 160.302 (Compliance and Enforcement) to apply to HIPAA privacy and security rule generally. Modified the definition to include reference to business associates	
	Standard means a rule, condition, or requirement: (1) Describing the following information for products, systems, services, or practices: (i) Classification of components; (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of protected health information.	*Standard* means a rule, condition, or requirement: (1) Describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of individually identifiable health information.	Revised the wording from reference to "individually identifiable health information" to "protected health information" in order to be more consistent with applicability of standards under HITECH.	
	State refers to one of the following: (1) For a health plan established or	*State* refers to one of the following: (1) For a health plan established or regulated	Added additional U.S. territories to the definition of "State" to be more consistent	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan. (2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.	by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan. (2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.	with the definition under HITECH.	
	Subcontractor means a person 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.	NEW	Added new definition to specify who is considered a Subcontractor for purposes of the HIPAA regulations.	
	Violation or violate means, as the context may require, failure to comply with an administrative simplification provision.	*Violation* or *violate* means, as the context may require, failure to comply with an administrative simplification provision.	Moved this definition from § 160.302 (Compliance and Enforcement) to apply to HIPAA privacy and security rule generally. No substantive changes to the definition.	
	Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.	*Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.	Modified the definition to include reference to business associates.	
5	Add § 160.105 to subpart A to read as follows: **§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.** Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and	NEW	Added a new subsection to address the applicable compliance date for all new or modified standards and implementation specifications to be effective 180 from the effective date as specified in the final rule following publication of the final rule in the federal register.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.			
6	Revise § 160.201 to read as follows: **§ 160.201 Statutory basis.** The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.	**§ 160.201 Applicability.** The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104–191.	Modified the statutory basis of Subpart B-Preemption of State Law to include a reference to the relevant section of the HITECH Act,	
7	In § 160.202, revise the definition of "Contrary" and paragraph (1)(i) of the definition of "More stringent" to read as follows: **§ 160.202 Definitions.**			
	Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means: (1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law. 104-191, or sections 13400 – 13424 of Public Law 111-5, as applicable.	*Contrary*, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means: (1) A covered entity would find it impossible to comply with both the State and federal requirements; or (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104–191, as applicable.	Modified the definition to include reference to business associates and also reference to the additional authority under the HITECH Act	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	More stringent * * * (1) * * * (i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or * * * *	*More stringent* * * * (1) * * * (i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or * * * *	Modified the definition to include reference to business associates.	
8	Revise § 160.300 to read as follows: **§ 160.300 Applicability.** This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.	**§ 160.300 Applicability.** This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.	Modified the applicability of the "Subpart C-Compliance and Investigations" to include reference to business associates as applicable entities.	
9	**§ 160.302 [Removed and Reserved]** Remove and reserve § 160.302.		Definitions in this subsection have been moved to § 160.103 to be applicable to HIPAA privacy and security generally, and not just "Compliance and Investigations". The definitions moved are: *Administrative simplification provision*, *ALJ*, *Civil money penalty*, *Respondent*, and *Violation or Violate*.	
10	Revise § 160.304 to read as follows: **§ 160.304 Principles for achieving compliance.** (a) Cooperation. The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions. (b) Assistance. The Secretary may provide technical assistance to covered entities and business associates to help them comply	**§ 160.304 Principles for achieving compliance.** (a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable administrative simplification provisions. (b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable administrative simplification provisions.	Modified the subsection to include reference to business associates as applicable entities.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	voluntarily with the applicable administrative simplification provisions.			
11	In § 160.306, revise paragraphs (a) and (c) to read as follows: **§ 160.306 Complaints to the Secretary.** (a) Right to file a complaint. A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary. * * * * * (c) Investigation. (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect. (2) The Secretary may investigate any other complaint filed under this section. (3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation. (4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.	**§ 160.306 Complaints to the Secretary.** (a) *Right to file a complaint.* A person who believes a covered entity is not complying with the administrative simplification provisions may file a complaint with the Secretary. * * * * * (c) *Investigation*. The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged violation. At the time of initial written communication with the covered entity about the complaint, the Secretary will describe the act(s) and/or omission(s) that are the basis of the complaint.	Modified the subsection to include reference to business associates as applicable entities for complaints to the secretary and investigations by the secretary. Also, inserted a new paragraph (1) in subsection (c) Investigation, to address the circumstances when the secretary must, in accordance with HITECH, investigate a complaint when a preliminary review of the facts indicates a possible violation due to willful neglect.	
12	Revise § 160.308 to read as follows: **§ 160.308 Compliance reviews.** (a) The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect. (b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the	**§ 160.308 Compliance reviews.** The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable administrative simplification provisions.	Modified the subsection to include reference to business associates as applicable entities for compliance reviews by the secretary. Also, inserted a new paragraph (a) to address the circumstances when the secretary must, in accordance with HITECH, conduct a compliance review when a preliminary review of the facts indicates a possible violation due to willful neglect.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	applicable administrative simplification provisions in any other circumstance.			
13	Revise § 160.310 to read as follows: **§ 160.310 Responsibilities of covered entities and business associates.** (a) Provide records and compliance reports. A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions. (b) Cooperate with complaint investigations and compliance reviews. A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions. (c) Permit access to information. (1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice. (2) If any information required of a covered entity or business associate under this section	**§ 160.310 Responsibilities of covered entities.** (a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable administrative simplification provisions. (b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity to determine whether it is complying with the applicable administrative simplification provisions. (c) *Permit access to information.* (1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice. (2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.	Modified the subsection to include reference to business associates with respect to providing records and reports to the secretary, or otherwise cooperating with complaints and/or investigations.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information. (3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).	(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, or if otherwise required by law.		
14	Revise § 160.312 to read as follows: **§ 160.312 Secretarial action regarding complaints and compliance reviews.** (a) Resolution when noncompliance is indicated. (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement. (2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing. (3) If the matter is not resolved by informal means, the Secretary will – (i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under	**§ 160.312 Secretarial action regarding complaints and compliance reviews.** (a) *Resolution when noncompliance is indicated.* (1) If an investigation of a complaint pursuant to §160.306 or a compliance review pursuant to §160.308 indicates noncompliance, the Secretary will attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement. (2) If the matter is resolved by informal means, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing. (3) If the matter is not resolved by informal means, the Secretary will— (i) So inform the covered entity and provide the covered entity an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§160.408 and 160.410 of this part. The covered entity must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under	Modified the subsection to include reference to business associates with respect to resolution of complaints, investigations or compliance reviews.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	§§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and (ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part. (b) Resolution when no violation is found. If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.	§160.526 of this part) of receipt of such notification; and (ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity of such finding in a notice of proposed determination in accordance with §160.420 of this part. (b) *Resolution when no violation is found.* If, after an investigation pursuant to §160.306 or a compliance review pursuant to §160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing.		
15	In § 160.316, revise the introductory text to read as follows: **§ 160.316 Refraining from intimidation or retaliation.** A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for – * * * * *	**§ 160.316 Refraining from intimidation or retaliation.** A covered entity may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for— * * * * *	Modified the subsection to include reference to business associates with respect to the requirement to refrain from intimidation or retaliation against individuals who report/complain.	
16	In § 160.401, revise the definition of reasonable cause to read as follows: **§ 160.401 Definitions.** * * * * * Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification	*Reasonable cause* means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.	Modified the definition to include reference to business associates and to align the culpability definition with HITECH.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	provision, but in which the covered entity or business associate did not act with willful neglect.			
17	Revise § 160.402 to read as follows: **§ 160.402 Basis for a civil money penalty.** (a) General rule. Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision. (b) Violation by more than one covered entity or business associate. (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate. (2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter 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. (c) Violation attributed to a covered entity or business associate. (1) A covered entity is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency. (2) A business associate is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a	**§ 160.402 Basis for a civil money penalty.** (a) *General rule.* Subject to §160.410, the Secretary will impose a civil money penalty upon a covered entity if the Secretary determines that the covered entity has violated an administrative simplification provision. (b) *Violation by more than one covered entity.* (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity. (2) A covered entity that is a member of an affiliated covered entity, in accordance with §164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter 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. (c) *Violation attributed to a covered entity.* A covered entity is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member, acting within the scope of the agency, unless— (1) The agent is a business associate of the covered entity; (2) The covered entity has complied, with respect to such business associate, with the applicable requirements of §§164.308(b) and 164.502(e) of this subchapter; and (3) The covered entity did not— (i) Know of a pattern of activity or practice of the business associate, and (ii) Fail to act as required by	Modified the subsection to include reference to business associates with respect to the basis for imposing a civil monetary penalty for violation of any administrative simplification provisions.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	workforce member or subcontractor, acting within the scope of the agency.	§§164.314(a)(1)(ii) and 164.504(e)(1)(ii) of this subchapter, as applicable.		
18	In § 160.404, revise the introductory text of paragraphs (b)(2)(i), (b)(2)(iii), and (b)(2)(iv) to read as follows: **§ 160.404 Amount of a civil money penalty.** * * * * * (b) * * * (2) * * * (i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, * * * * * (iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, * * * * * (iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, * * * * *	**§ 160.404 Amount of a civil monetary penalty.** * * * * * (b) * * * (2) * * * (i) For a violation in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision, * * * * * (iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, * * * * * (iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, * * * * *	Modified the subsection to include reference to business associates with respect to the levels of culpability which may form the basis for the amount of civil monetary penalty to be imposed under HITECH.	
19	Revise § 160.406 to read as follows: **§ 160.406 Violations of an identical requirement or prohibition.** The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to	**§ 160.406 Violations of an identical requirement or prohibition.** The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within	Modified the subsection to include reference to business associates with respect to considering identical violations for determining the extent of civil monetary penalties to be imposed.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.	a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity is in violation of the provision.		
20	Revise § 160.408 to read as follows: **§160.408 Factors considered in determining the amount of a civil money penalty.** In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate: (a) The nature and extent of the violation, consideration of which may include but is not limited to: (1) The number of individuals affected; and (2) The time period during which the violation occurred; (b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to: (1) Whether the violation caused physical harm; (2) Whether the violation resulted in financial harm; (3) Whether the violation resulted in harm to an individual's reputation; and (4) Whether the violation hindered an individual's ability to obtain health care; (c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to: (1) Whether the current violation is the same or similar to previous indications of noncompliance; (2) Whether and to what extent the covered	**§ 160.408 Factors considered in determining the amount of a civil money penalty.** In determining the amount of any civil money penalty, the Secretary may consider as aggravating or mitigating factors, as appropriate, any of the following: (a) The nature of the violation, in light of the purpose of the rule violated. (b) The circumstances, including the consequences, of the violation, including but not limited to: (1) The time period during which the violation(s) occurred; (2) Whether the violation caused physical harm; (3) Whether the violation hindered or facilitated an individual's ability to obtain health care; and (4) Whether the violation resulted in financial harm. (c) The degree of culpability of the covered entity, including but not limited to: (1) Whether the violation was intentional; and (2) Whether the violation was beyond the direct control of the covered entity. (d) Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to: (1) Whether the current violation is the same or similar to prior violation(s); (2) Whether and to what extent the covered entity has attempted to correct previous	Modified this section to reorganize the factors to consider in determining the amount of civil monetary penalty pursuant to the requirements of the HITECH Act, and also to include reference to the applicability of the subsection to business associates. The majority of the factors remain unchanged, despite the reorganization and/or the order of the factors to be considered.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	entity or business associate has attempted to correct previous indications of noncompliance; (3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and (4) How the covered entity or business associate has responded to prior complaints; (d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to: (1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply; (2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and (3) The size of the covered entity or business associate; and (e) Such other matters as justice may require.	violations; (3) How the covered entity has responded to technical assistance from the Secretary provided in the context of a compliance effort; and (4) How the covered entity has responded to prior complaints. (e) The financial condition of the covered entity, including but not limited to: (1) Whether the covered entity had financial difficulties that affected its ability to comply; (2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and (3) The size of the covered entity. (f) Such other matters as justice may require.		
21	Revise § 160.410 to read as follows: **§160.410 Affirmative defenses.** (a) The Secretary may not: (1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d-6. (2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.	**§ 160.410 Affirmative defenses.** (a) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violations, including the following: (1) The violation is an act punishable under 42 U.S.C. 1320d–6; (2) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the federal common law of agency, and, by exercising reasonable diligence, would not have known that the violation occurred; or (3) The violation is—	Inserted new subsection (a) to clarify the requirement under HITECH that the secretary may not impose a civil penalty that is criminally punishable (prior to 2/18/2011), or otherwise if the violating entity can show that a criminal penalty has been imposed (on or after 2/18/2011). Also removed the words. “reasonable cause” in (a)(3)(i) and instead inserted the textual definition of reasonable cause in the new section (b)(2)(i).	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following: (1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or (2) The violation is – (i) 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 administrative simplification provision violated and is not due to willful neglect; and (ii) Corrected during either: (A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or (B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply. (c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is – (1) Not due to willful neglect; and (2) Corrected during either: (i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that	(i) Due to reasonable cause and not willful neglect; and (ii) Corrected during either: (A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or (B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply. (b) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violations, including the following: (1) The violation is an act punishable under 42 U.S.C. 1320d–6; or (2) The covered entity establishes to the satisfaction of the Secretary that the violation is— (i) Not due to willful neglect; and (ii) Corrected during either: (A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or (B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	the violation occurred; or (ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.			
22	Revise § 160.412 to read as follows: **§ 160.412 Waiver.** For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.	**§ 160.412 Waiver.** For violations due to reasonable cause and not willful neglect that are not corrected within the period described in § 160.410(a)(3)(ii) or (b)(2)(ii), as applicable, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.	Modified the waiver provision to conform to the modified sections in the above civil penalty provisions.	
23	Revise § 160.418 to read as follows: **§ 160.418 Penalty not exclusive.** Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1) and 42 U.S.C. 299b-22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.	**§ 160.418 Penalty not exclusive.** Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1), a penalty imposed under this part is in addition to any other penalty prescribed by law.	Added reference to the penalty provision of the Patient Safety and Quality Improvement Act which provides that penalties are not be imposed under both that act and HIPAA for the same violation.	
24	Amend § 160.534 as follows: a. Revise paragraph (b)(1)(iii); b. Add paragraph (b)(1)(iv); and c. Revise paragraph (b)(2). The revisions read as follows: **§160.534 The hearing.** * * * * * (b)(1) * * * (iii) Claim that a proposed penalty should be reduced or waived pursuant to § 160.412 of this part; and (iv) Compliance with subpart D of part 164, as provided under §164.414(b). (2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed	**§ 160.534 The hearing.** * * * * * (b)(1) * * * (iii) Claim that a proposed penalty should be reduced or waived pursuant to §160.412 of this part. (2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability and the existence of any factors considered as aggravating factors in determining the amount of the proposed penalty. * * * * *	Modified the burden of persuasion obligation during enforcement hearings to establish that the respondent has the burden of proof and persuasion for investigations involving the breach notification rule.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	penalty. * * * * *			
25	The authority citation for part 164 is revised to read as follows: **Authority:** 42 U.S.C. 1302(a); 42 U.S.C. 1320d – 1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); and secs. 13400 - 13424, Pub. L. 111-5, 123 Stat. 258-279.	**Authority:** 42 U.S.C. 1320d–1320d–8 and sec. 264, Pub. L. No. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)).	Added reference to HITECH as additional authority for implementing the HIPAA privacy and security regulations, generally.	
26	Revise § 164.102 to read as follows: **§ 164.102 Statutory basis.** The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and sections 13400 – 13424 of Public Law 111-5.	**§ 164.102 Statutory basis.** The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act and section 264 of Public Law 104–191.	Added reference to HITECH as an additional statutory basis for implementing required regulations.	
27	In § 164.104, revise paragraph (b) to read as follows: **§ 164.104 Applicability.** * * * * * (b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.	**§ 164.104 Applicability.** * * * * * (b) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, or other than as a business associate of a covered entity, the clearinghouse must comply with §164.105 relating to organizational requirements for covered entities, including the designation	Revised paragraph (b) to indicate that certain standards, requirements and implementation specifications will apply to business associates (as well as covered entities, which are identified in paragraph (a)).	
28	Amend § 164.105 as follows: a. Revise the introductory text of paragraph (a)(1), the introductory text of paragraph (a)(2)(i), paragraph (a)(2)(ii), the introductory text of paragraph (a)(2)(iii), and paragraphs (a)(2)(iii)(A) and (B); b. Redesignate paragraph (a)(2)(iii)(C) as paragraph (a)(2)(iii)(D) and add new paragraph (a)(2)(iii)(C); c. Revise newly redesignated paragraph	**§ 164.105 Organizational requirements.** (a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, §164.314, and §164.504, apply only to the health care component(s) of the entity, as specified in this section. (2) * * * (i) *Application of other provisions.* In	Several modifications to this section were made to remove references to subparts C and E so as to conform the rules to not exclude subpart D which was added to include the breach notification rules. Instead, the rules now refer to "this part" generally. Also, deleted paragraphs C and D from subsection (a)(2)(ii) to remove unnecessary provisions that spell out a covered entity's obligation to ensure	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(a)(2)(iii)(D); and d. Revise paragraph (b). The revisions read as follows: **§ 164.105 Organizational requirements.** (a)(1) Standard: Health care component. If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section. (2) * * * (i) Application of other provisions. In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity: * * * * * (ii) Safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that: (A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities; (B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities; (C) If a person performs duties for both the	applying a provision of subparts C and E of this part, other than the requirements of this section, §164.314, and §164.504, to a hybrid entity: * * * * * (ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that: (A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities; (B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities; (C) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by subpart E of this part; (D) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section that creates, receives, maintains, or transmits electronic protected health information on behalf of the health care component is in compliance with subpart C of this part; and (E) If a person performs duties for both the	that any component that performs business associate-like activities and is included in its healthcare component complies with privacy and security rules. These sections are no longer necessary since business associates are subject to direct enforcement under HITECH. In addition, collapsed the paragraphs in subsection (b)(2)(ii) to simplify the provision that outlines requirements of affiliated entities to comply with privacy and security rules.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part. (iii) Responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities: (A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part. (B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section. (C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements. (D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions. (b)(1) Standard: Affiliated covered entities.	health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part. (iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities: (A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with subpart E of this part. (B) The covered entity is responsible for complying with §164.316(a) and §164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this section and subparts C and E of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section. (C) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs: (1) Covered functions; or (2) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part. (2) Implementation specifications. (i) Requirements for designation of an affiliated covered entity. (A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control. (B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section. (ii) Safeguard requirements. An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable. * * * * *	entities. (b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part. (2) *Implementation specifications:* (i) *Requirements for designation of an affiliated covered entity.* (A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of subparts C and E of this part, if all of the covered entities designated are under common ownership or control. (B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section. (ii) *Safeguard requirements.* An affiliated covered entity must ensure that: (A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part; (B) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of subpart E of this part; and (C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with §164.308(a)(4)(ii)(A) and §164.504(g), as applicable. * * * * *		
29	Revise § 164.106 to read as follows: **§ 164.106 Relationship to other parts.** In complying with the requirements of this	**§ 164.106 Relationship to other parts.** In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160	Modified the subsection to include reference to business associates as applicable entities relative to the provision.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.	and 162 of this subchapter.		
30	The authority citation for subpart C of part 164 is revised to read as follows: Authority: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.	**Authority:** 42 U.S.C. 1320d-2 and 1320d-4.	Added reference to HITECH as additional authority for implementing the HIPAA security regulations, generally.	
31	Revise § 164.302 to read as follows: **§ 164.302 Applicability.** A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.	**§ 164.302 Applicability.** A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.	Revised the paragraph to indicate that applicable standards, requirements and implementation specifications will apply to business associates (as well as covered entities, as required under HITECH).	
32	In § 164.304, revise the definitions of Administrative safeguards and Physical safeguards to read as follows: **§ 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 or business associate's workforce in relation to the protection of that information.	*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.	Modified the definition to include reference to business associates.	
	Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and	*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.	Modified the definition to include reference to business associates.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	unauthorized intrusion.			
33	Amend § 164.306 as follows: a. Revise the introductory text of paragraph (a) and paragraph (a)(1); b. Revise paragraph (b)(1), the introductory text of paragraph (b)(2), and paragraphs (b)(2)(i) and (b)(2)(ii); c. Revise paragraph (c); d. Revise paragraph (d)(2), the introductory text of paragraph (d)(3), paragraph (d)(3)(i), and the introductory text of paragraph (d)(3)(ii); and e. Revise paragraph (e). The revisions read as follows: **§ 164.306 Security standards: General rules.** (a) General requirements. Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. * * * * * (b) * * * (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. * * * * *	**§ 164.306 Security standards: General rules.** (a) *General requirements.* Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. * * * * * (b) * * * (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The covered entity's technical infrastructure, hardware, and software security capabilities. * * * * * (c) *Standards.* A covered entity must comply with the standards as provided in this section and in §164.308, §164.310, §164.312, §164.314, and §164.316 with respect to all electronic protected health information. (d) * * * (2) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (3) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity must— (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed	Modified the subsection to include reference to business associates as applicable entities relative to the provision.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(c) Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information. (d) * * * (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications. (3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must – (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and (ii) As applicable to the covered entity or business associate – * * * * * (e) Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).	with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity— * * * * * (e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at §164.316.		
34	Amend § 164.308 as follows: a. Revise the introductory text of paragraph (a), paragraph (a)(1)(ii)(A), paragraph (a)(1)(ii)(C), paragraph (a)(2), paragraph (a)(3)(ii)(C), paragraph (a)(4)(ii)(C), paragraph (a)(6)(ii), and paragraph (a)(8); and b. Revise paragraph (b).	**§ 164.308 Administrative safeguards.** (a) A covered entity must, in accordance with §164.306: (1) * * * (ii) * * * (A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the	Modified the subsection to include reference to business associates as applicable entities relative to several part of the provision. Also included reference to the business associate's obligation to enter into written business associate agreements with subcontractors and	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	The revisions read as follows: **§ 164.308 Administrative safeguards.** (a) A covered entity or business associate must, in accordance with § 164.306: (1) * * * (ii) * * * (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. * * * * * (C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. * * * * * (2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. (3) * * * (ii) * * * (C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. (4) * * * (ii) * * * (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered	potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. * * * * * (C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. * * * * * (2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. (3)(i) * * * (ii) * * * (C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. (4)(i) * * * (ii) * * * (C) *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. * * * * * (6)(i) * * * (ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document	clarification that the covered entity is not required to enter business associate agreements with the subcontractors of the covered entity's business associates. In addition, removed some subsections as unnecessary with respect to activities that are not applicable to the standard.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. * * * * * (6) * * * (ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. * * * * * (8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. (b)(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its	security incidents and their outcomes. * * * * * (8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. (b)(1) *Standard: Business associate contracts and other arrangements.* A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information. (2) This standard does not apply with respect to— (i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual. (ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) and §164.504(f) apply and are met; or (iii) The transmission of electronic protected health information from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. (3) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	requirements of §164.502(e)(1)(ii)(C) are met. (3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a). (4) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).		
35	Revise the introductory text of § 164.310 to read as follows: **§ 164.310 Physical safeguards.** A covered entity or business associate must, in accordance with § 164.306: * * * * *	**§ 164.310 Physical safeguards.** A covered entity must, in accordance with §164.306:	Modified the introductory section to include the applicability of the provisions to business associates as required under HITECH.	
36	Revise the introductory text of § 164.312 to read as follows: **§ 164.312 Technical safeguards.** A covered entity or business associate must, in accordance with § 164.306:	**§ 164.312 Technical safeguards.** A covered entity must, in accordance with §164.306:	Modified the introductory section to include the applicability of the provisions to business associates as required under HITECH.	
37	Amend § 164.314 by revising paragraphs (a) and (b)(2)(iii) to read as follows: **§ 164.314 Organizational requirements.** (a)(1) Standard: Business associate contracts or other arrangements. The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable. (2) Implementation specifications (Required). (i) Business associate contracts. The contract must provide that the business associate will –	**§ 164.314 Organizational requirements.** (a)(1) *Standard: Business associate contracts or other arrangements.* (i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material	Revised this section by removing the provisions at (a)(1)(ii) regarding the steps a covered entity must take if it knows of a material breach or violation by its business associate because a parallel provision exists in the privacy rule at § 164.504. The duplicate provisions are therefore unnecessary. Also, the revisions seek to streamline the provision to simply indicate the business associates' obligation to security rule, and added language outlining the business associate's obligation to contract with	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410. (ii) Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3). (iii) Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. (b) * * * (2) * * * (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and * * * * *	breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful— (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary. (2) *Implementation specifications (Required).* (i) *Business associate contracts.* The contract between a covered entity and a business associate must provide that the business associate will— (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (ii) *Other arrangements.* (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if— (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted	subcontractors to require compliance with the security rule. In addition, removed reference to subcontractors regarding group health plan documents as a condition of disclosure of PHI to plan sponsor in order to avoid confusion with the use of the term, subcontractor as related to business associates.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
		by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. (B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. (b) * * * (2) * * * (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and * * * * *		
38	Revise the introductory text of § 164.316 and the third sentence of paragraph (a) to read as follows:	**§ 164.316 Policies and procedures and documentation requirements.** A covered entity must, in accordance with §164.306:	Modified the introductory section to include the applicability of the provisions to business associates as required under HITECH.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	§ 164.316 Policies and procedures and documentation requirements. A covered entity or business associate must, in accordance with § 164.306: (a) * * * A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. * * * * *	(a) * * *. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.		
39	Revise § 164.402 to read as follows: **§ 164.402 Definitions.** As used in this subpart, the following terms have the following meanings:			
	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized	*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. (2) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person	Definition of Breach has been modified to remove the risk of harm exception and instead requires a more objective standard to conduct a risk analysis to assess whether there is a likelihood that the PHI breached has been compromised.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E 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 based on a risk assessment of at least the following 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.	who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.		
	Unsecured protected health information means protected health	*Unsecured protected health information* means protected health information that is not	Definition slightly modified to remove reference to the HHS website.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.	rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS web site.		
40	In § 164.406, revise paragraph (a) to read as follows: **§ 164.406 Notification to the media.** (a) Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. * * * * *	**§ 164.406 Notification to the media.** (a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.	Removed reference to American Samoa and the Northern Mariana Islands as these have been included in the definition of "State."	
41	In § 164.408, revise paragraph (c) to read as follows: **§ 164.408 Notification to the Secretary.** * * * * * (c) Implementation specifications: Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.	**§ 164.408 Notification to the Secretary.** * * * * * (c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site.	Modified provision to clarify that annual reporting is required for breaches *discovered* in the previous calendar year versus breaches that *occurred* in the previous calendar year.	
42	In § 164.410, revise paragraph (a) to read as follows: **§ 164.410 Notification by a business associate.**	**§ 164.410 Notification by a business associate.** (a) *Standard.* (1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify	Technical, non-substantive changes.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(a) Standard—(1) General rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency). * * * * *	the covered entity of such breach. (2) *Breaches treated as discovered.* For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).		
43	The authority citation for subpart E of part 164 is revised to read as follows: Authority: 42 U.S.C.1320d-2 and 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); and secs. 13400 – 13424, Pub. L. 111-5, 123 Stat. 258-279.	Authority: 42 U.S.C.1320d-2 and 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note));	Added reference to HITECH as additional authority for implementing the HIPAA privacy regulations, generally.	
44	In § 164.500, redesignate paragraph (c) as paragraph (d) and add new paragraph (c) to read as follows: **§ 164.500 Applicability.** * * * * * (c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity. * * * * *	NEW	Inserted new provision to indicate that, where provided, certain standards, requirements and implementation specifications of the privacy rule will apply to business associates as required under HITECH.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
45	Amend § 164.501 as follows: a. Revise paragraph (1) and (3) of the definition of "Health care operations"; b. Revise the definition of "Marketing"; and c. Revise paragraph (1)(i) of the definition of "Payment". The revisions read as follows: **§ 164.501 Definitions.**			
	Health care operations * * * (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; * * * * * (3) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided	*Health care operations* * * * (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; * * * * * (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; * * * * *	Revised the definition to include patient safety activities within the definition of health care operations	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	that the requirements of §164.514(g) are met, if applicable; * * * * *			
	Marketing: (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. (2) Marketing does not include a communication made: (i) For treatment of an individual by a health care provider, including 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, provided, however, that if the communication is in writing and the health care provider receives financial remuneration in exchange for making the communication, the requirements of § 164.514(f)(2) are met. (ii) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. (iii) For the following health care operations activities, except where the covered entity receives financial remuneration in exchange for making the communication: (A) To describe a health-related	*Marketing* means: (1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is 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, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. (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. (2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.	Revised the definition of marketing to be consistent with limitations provided under HITECH with respect to unauthorized communications to individuals generally, and particularly limiting the circumstances that such communications may occur in exchange for direct or indirect remuneration.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	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, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (B) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment. (3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual. * * * * *			
	Payment means: (1) * * * (i) Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or * * * * *	*Payment* means: (1) * * * (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or * * * * *	Added exception for prohibition relative to health coverage premium payments under GINA.	
46	In § 164.502, revise paragraphs (a), (b)(1), (e), and (f) to read as follows: **§ 164.502 Uses and disclosures of protected**	**§ 164.502 Uses and disclosures of protected health information: general rules.** (a) *Standard.* A covered entity may not use or disclose protected health information, except	Revised this subsection to clarify the obligations applicable to covered entities and added companion provisions applicable to business associates relative	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	health information: General rules. (a) Standard. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter. (1) Covered entities: Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows: (i) To the individual; (ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure; (iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508; (v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and (vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g). (2) Covered entities: Required disclosures. A covered entity is required to disclose protected health information: (i) To an individual, when requested under, and required by § 164.524 or § 164.528; and (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter. (3) Business associates: Permitted uses and disclosures. (i) A business associate may use or disclose protected health information only	as permitted or required by this subpart or by subpart C of part 160 of this subchapter. (1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows: (i) To the individual; (ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502(b), §164.514(d), and §164.530(c) with respect to such otherwise permitted or required use or disclosure; (iv) Pursuant to and in compliance with a valid authorization under §164.508; (v) Pursuant to an agreement under, or as otherwise permitted by, §164.510; and (vi) As permitted by and in compliance with this section, §164.512, or §164.514(e), (f), or (g). (2) *Required disclosures.* A covered entity is required to disclose protected health information: (i) To an individual, when requested under, and required by §164.524 or §164.528; and (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart. (b) * * * (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. * * * * *	to uses and disclosures of PHI. Also, removed as unnecessary provisions exclusions of this provision to certain disclosures between covered entities and business associates due to the fact that business associates are now subject to direct enforcement under HIPAA. Required Disclosures for business associates defined. Prohibited uses and disclosures added as required under GINA. In addition, included language that permits business associates to disclosure PHI to subcontractors and limiting the covered entity obligation to contract directly with subcontractors of business associates. Finally, added in language that removes limitation of disclosure regarding individuals deceased for more than 50 years.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e), or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement. (4) Business associates: Required uses and disclosures. A business associate is required to disclose protected health information: (i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter. (ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information. (5) Prohibited uses and disclosures. (i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including	(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. (ii) This standard does not apply: (A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual; (B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of §164.504(f) apply and are met; or (C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan. (iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	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); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. (B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy. (ii) Sale of protected health information: (A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information. (B) For purposes of this paragraph, sale of protected health information means: (1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information. (2) Sale of protected health information does not include a disclosure of protected health information: (i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);	§164.504(e). (2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e). (f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual. * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes; (iii) For treatment and payment purposes pursuant to § 164.506(a); (iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a); (v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities; (vi) To an individual, when requested under § 164.524 or § 164.528; (vii) Required by law as permitted under § 164.512(a); and (viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law. (b) * * * (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information			

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. * * * * * (e)(1) Standard: Disclosures to business associates. (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. (ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create or receive protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. (2) Implementation specification: Documentation. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e). (f) Standard: Deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of			

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	the individual. * * * * *			
47	In § 164.504, revise paragraphs (e), (f)(1)(ii) introductory text, and (f)(2)(ii)(B) to read as follows: **§ 164.504 Uses and disclosures: Organizational requirements.** * * * * * (e)(1) Standard: Business associate contracts. (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. (iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. (2) Implementation specifications: Business associate contracts. A contract between the covered entity and a business associate must: (i) Establish the permitted and required uses	**§ 164.504 Uses and disclosures: Organizational requirements.** * * * * * (e)(1) Standard: Business associate contracts. (i) The contract or other arrangement between the covered entity and the business associate required by §164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary. (2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must: (i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that: (A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section;	Revised several requirements with respect to business associate contracts. First, added subsection (e)(1)(iii) to establish noncompliance of business associate if the business associate knew of a pattern of activity by its subcontractors in material breach of the agreement. Also removed the provision requiring a covered entity to report breaches of business associates to the secretary as unnecessary because business associate is now already subject to direct enforcement under HITECH. Also, added reference to the business associate agreement provisions to require notification of breaches of PHI under the breach notification rule. In addition, inserted a new provision at (e)(2)(ii)(H) that requires business associate agreement to include a provision that business associate must comply with the privacy rule to the extent the applicable to the business associate's contracted activities to carry out the obligations of the covered entity. Added a new provision at (e)(3)(iv) that allows a covered entity that shares only a limited data set with a business associate to execute a data use agreement rather than a business associate agreement. Also, added a new provision (e)(5) that requires that all requirements for business associate agreements that apply to covered entities are equally applicable to business associates. Finally, removed reference to the term subcontractor in provision about disclosures of PHI to plan sponsor of a group health plan in order to avoid confusion with the term subcontractor as it relates to business associates.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that: (A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and (B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity. (ii) Provide that the business associate will: (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law; (B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract; (C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410; (D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain or transmit 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; (E) Make available protected health information in accordance with § 164.524; (F) Make available protected health	and (B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity. (ii) Provide that the business associate will: (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law; (B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract; (C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware; (D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information; (E) Make available protected health information in accordance with §164.524; (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with §164.528; (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (I) At termination of the contract, if feasible, return or destroy all protected health		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	information for amendment and incorporate any amendments to protected health information in accordance with § 164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528; (H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation. (I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. (iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (3) Implementation specifications: Other arrangements. (i) If a covered entity and its business associate are both governmental entities: (A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of	information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. (iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities: (A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section. (B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section. (ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in §160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable. (B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable. (ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained. (iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. (iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement	in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained. (iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. (4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary: (A) For the proper management and administration of the business associate; or (B) To carry out the legal responsibilities of the business associate. (ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if: (A) The disclosure is required by law; or (B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and (2) The person notifies the business associate of any instances of which it is aware in which		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable. (4) Implementation specifications: Other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary: (A) For the proper management and administration of the business associate; or (B) To carry out the legal responsibilities of the business associate. (ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if: (A) The disclosure is required by law; or (B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and (2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached. (5) Implementation specifications: Business associate contracts with subcontractors. The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as	the confidentiality of the information has been breached. (f)(1) * * * (ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of : * * * * * (2) * * * (ii) * * * (B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	such requirements apply to contracts or other arrangements between a covered entity and business associate. (f)(1) * * * (ii) Except as prohibited by §164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of: * * * * * (2) * * * (ii) * * * (B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; * * * * *			
48	In § 164.506, revise paragraphs (a) and (c)(5) to read as follows: **§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.** (a) Standard: Permitted uses and disclosures. Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) through (4) or that are prohibited under §164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart. * * * * * (c) * * * (5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the	**§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.** (a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart. * * * * * (c) * * * (5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.	Revised the allowable uses and disclosures of PHI by a covered entity include requirements under GINA and to clarify that allowable disclosures include to other "participants" in an organized health care arrangement rather than just "another covered entity" participant to recognize that there may be participants to whom disclosure is necessary that are not themselves covered entities	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	organized health care arrangement for any health care operations activities of the organized health care arrangement.			
49	Amend § 164.508 as follows: a. Revise the headings of paragraphs (a), (a)(1), and (a)(2); b. Revise paragraph (a)(3)(ii); c. Add new paragraph (a)(4); and d. Revise paragraphs (b)(1)(i), and (b)(3). The revisions and additions read as follows: **§ 164.508 Uses and disclosures for which an authorization is required.** (a) Standard: Authorizations for uses and disclosures—(1) Authorization required: General rule. * * * (2) Authorization required: Psychotherapy notes. * * * (3) * * * (ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved. (4) Authorization required: Sale of protected health information. (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity. (b) * * * (1) * * * (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this	**§ 164.508 Uses and disclosures for which an authorization is required.** (a) *Standard: Authorizations for uses and disclosures* (1) *Authorization required: General rule.* * * * (2) *Authorization required: Psychotherapy notes.* * * * (3) * * * (ii) If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. (b) * * * (1) * * * (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable. * * * * * (3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows: (i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research; (ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; (iii) An authorization under this section, other than an authorization for a use or	Revised this section to insert new requirement that authorization to disclose PHI is required when the covered entity receives financial remuneration in exchange for the disclosure and also spells out the types of disclosures that are inapplicable to this requirement. Also, the rule is modified to further clarify the requirements to delineate whenever compound authorizations (a single authorization for more than one purpose) are obtained.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	section, as applicable. * * * * * (3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows: (i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization. (ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes. (iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such 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 under paragraph (b)(4)	disclosure of psychotherapy notes, may be combined with any other such 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 under paragraph (b)(4) of this section on the provision of one of the authorizations. * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section. * * * * *			
50	Amend § 164.510 as follows: a. Revise paragraph (a)(1)(ii) introductory text; b. Revise paragraph (b)(1)(i), the second sentence of paragraph (b)(1)(ii), paragraph (b)(2)(iii), the first sentence of paragraph (b)(3), and paragraph (b)(4); and c. Add new paragraph (b)(5). The revisions and additions read as follows: **§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.** * * * * * (a) * * * (1) * * * (ii) Use or disclose for directory purposes such information: * * * * * (b) * * * (1) * * * (i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health	**§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.** * * * * * (a) * * * (1) * * * (ii) Disclose for directory purposes such information: * * * * * (b) * * * (1) * * * (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. (ii) * * * Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable. * * * * * (2) * * * (iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual	Minor revisions to correct typographical issues and to update references to conform to other modified sections of the regulations. Also, added a provision allowing a covered entity to disclose PHI to certain family members and close friends of a deceased individual if such people were involved in the health care decisions of the individual prior to the individual's death – unless doing so would be contrary to any expressed preference of the individual and is known to the covered entity.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	care. (ii) * * * Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable. * * * * * (2) * * * (iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. (3) * * * If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. * * * (4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances. (5) Uses and disclosures when the individual	does not object to the disclosure. (3) * * * If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. * * * (4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances. (ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	is deceased. If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.			
51	Amend § 164.512 as follows: a. Revise the paragraph heading for paragraph (b), the introductory text of paragraph (b)(1) and the introductory text of paragraph (b)(1)(v)(A); b. Add new paragraph (b)(1)(vi); c. Revise the introductory text of paragraph (e)(1)(iii) and paragraph (e)(1)(vi); d. Revise paragraph (i)(2)(iii); and e. Revise paragraphs (k)(1)(ii), (k)(3), and (k)(5)(i)(E). The revisions and additions read as follows: **§164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.** * * * * * (b) Standard: Uses and disclosures for public health activities. (1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to: * * * * * (v) * * * (A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer: * * * * * (vi) A school, about an individual who is a	**§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.** * * * * * (b) *Standard: uses and disclosures for public health activities* (1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to: * * * (v) * * * (A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer: * * * * * (e) * * * (1) * * * (iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that: * * * * * * * * (vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph	Updated the subsection to correct a few typographical errors and to edit references to sections to conform to other modified sections in the regulations. Also, added a new provision at (b)(1)(vi) to permit certain disclosures of PHI relative to students for certain public health activities. Updated a reference to the Dept of Homeland Security since the Dept of Transportation is now part of that agency.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	student or prospective student of the school, if: (A) The protected health information that is disclosed is limited to proof of immunization; (B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and (C) The covered entity obtains the agreement to the disclosure from either: (1) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or (2) The individual, if the individual is an adult or emancipated minor. * * * * * (e) * * * (1) * * * (iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that: * * * * * * * * (vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section. * * * * * (i) * * * (2) * * * (iii) Protected health information needed. A	(e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section. * * * * * (i) * * * (2) * * * (iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section; * * * * * (k) * * * (1) * * * (ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs. * * * * * (3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section; * * * * * (k) * * * (1) * * * (ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs. * * * * * (3) Protective services for the President and others. A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879. * * * * * (5) * * * (i) * * * (E) Law enforcement on the premises of the correctional institution; or * * * * *	22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879. * * * * * (5) * * * (i) * * * (E) Law enforcement on the premises of the correctional institution; and * * * * *		
52	In § 164.514, revise paragraphs (e)(4)(ii)(C)(4) and (f) to read as follows: **§ 164.514 Other requirements relating to**	**§ 164.514 Other requirements relating to uses and disclosures of protected health information.** * * * * *	Modified several requirements related to fundraising activities of covered entities to include a provision that a covered entity may not use PHI for fundraising	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	uses and disclosures of protected health information. * * * * * (e) * * * (4) * * * (ii) * * * (C) * * * (4) Ensure that any agents to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and * * * * * (f) Fundraising communications. (1) Standard: Uses and disclosures for fundraising. Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508: (i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth; (ii) Dates of health care provided to an individual; (iii) Department of service information; (iv) Treating physician; (v) Outcome information; and (vi) Health insurance status. (2) Implementation specifications: Fundraising requirements. (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice of privacy practices. (ii) With each fundraising communication	(e) * * * (4) * * * (ii) * * * (C) * * * (4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and * * * * * (f)(1) *Standard: Uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of §164.508: (i) Demographic information relating to an individual; and (ii) Dates of health care provided to an individual. (2) *Implementation specifications: Fundraising requirements.* (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(B) is included in the covered entity's notice; (ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications. (iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications. (g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health	activities unless such is disclosed in its NPP. Also, with each fundraising communication, the covered entity must give the individual clear and conspicuous information about how to opt out of future communications, and if an individual elects to opt out of such communication, the covered entity may not send any such future communications. The covered entity may not condition treatment on the authorization to provide such communication to individuals. In addition, if the covered entity receives financial remuneration for use of PHI in marketing activities, this must also be disclosed in the NPP, and the individual must be given clear and conspicuous information on how to opt out of receiving any such communications. The method of opting out may not cause the individual any undue burden.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. (iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications. (iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(1)(ii)(B) of this section. (v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications. (g) Standard: uses and disclosures for underwriting and related purposes. If a health plan receives protected health information 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, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at §164.502(a)(5)(i) with respect to genetic information included in the protected health information. * * * * *	plan receives protected heath information 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, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law. * * * * *		
53	Amend § 164.520: a. Revise paragraphs (b)(1)(ii)(E), (b)(1)(iii), (b)(1)(iv)(A), (b)(1)(v)(A), (c)(1)(i)	**§ 164.520 Notice of privacy practices for protected health information.** * * * * *	Modified this subsection to identify new required changes to the NPP, in particular the requirement to provide notice	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	introductory text, and (c)(1)(i)(B); b. Remove paragraph (c)(1)(i)(C); and c. Add paragraph (c)(1)(v). The revisions and addition read as follows: **§ 164.520 Notice of privacy practices for protected health information.** * * * * * (b) * * * (1) * * * (ii) * * * (E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5). (iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable: (A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; (B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or (C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for	(b) * * * (1) * * * (ii) * * * (E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by §164.508(b)(5). (iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that: (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 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 a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan. (iv) * * * (A) 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; * * * * * (v) * * * (A) 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 respect to protected health information; * * * * * (c) * * *	regarding financial remuneration in exchange for disclosure of PHI for marketing activities, and the right of an individual to opt out of receiving such communications for marketing and fund raising. In addition, the NPP must include a notice that individuals may request restrictions on disclosures that the covered entity is not required to agree to the restrictions, except restrictions to a health plan for an item or service that has been paid in full out of pocket.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes. (iv) * * * (A) 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, except in case of a disclosure restricted under § 164.522(a)(1)(vi); * * * * * (v) * * * (A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information; * * * * * (c) * * * (1) * * * (i) A health plan must provide the notice: * * * * * (B) Thereafter, at the time of enrollment, to individuals who are new enrollees. * * * * * (v) If there is a material change to the notice: (A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section 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.	(1) * * * (i) A health plan must provide notice: * * * * * (B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and (C) Within 60 days of a material revision to the notice, to individuals then covered by the plan. * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice. * * * * *			
54	Amend § 164.522 as follows: a. Revise paragraph (a)(1)(ii); b. Add new paragraph (a)(1)(vi); and c. Revise the introductory text of paragraph (a)(2), and paragraphs (a)(2)(iii), and paragraph (a)(3). The revisions and additions read as follows: **§ 164.522 Rights to request privacy protection for protected health information.** (a)(1) * * * (ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction. * * * * * (vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual 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 protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full. (2) Implementation specifications: Terminating a restriction. A covered entity may terminate a restriction, if: * * * * * (iii) The covered entity informs the individual	**§ 164.522 Rights to request privacy protection for protected health information.** (a)(1) * * * (ii) A covered entity is not required to agree to a restriction. * * * * * (2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate its agreement to a restriction, if : * * * * * (iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual. (3) *Implementation specification: Documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with §164.530(j). * * * * *	Inserted new paragraph (a)(1)(vi) and related references regarding the requirement under HITECH that the covered entity must agree to a requested restriction of disclosure to a health plan if the PHI pertains solely to an item or service that a person other than a health plan has paid the covered entity in full.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	that it is terminating its agreement to a restriction, except that such termination is: (A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and (B) Only effective with respect to protected health information created or received after it has so informed the individual. (3) Implementation specification: Documentation. A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter. * * * * *			
55	Amend § 164.524 as follows: a. Remove paragraph (b)(2)(ii) and redesignate paragraph (b)(2)(iii) as paragraph (b)(2)(ii); b. Revise newly designated paragraph (b)(2)(ii); c. Revise paragraph (c)(2)(i); d. Redesignate paragraph (c)(2)(ii) as paragraph (c)(2)(iii); e. Add new paragraph (c)(2)(ii); f. Revise paragraphs (c)(3) and (c)(4)(i); g. Redesignate paragraphs (c)(4)(ii) and (c)(4)(iii) as paragraphs (c)(4)(iii) and (c)(4)(iv), respectively; and h. Add new paragraph (c)(4)(ii). The revisions and additions read as follows: **§ 164.524 Access of individuals to protected health information.** * * * * * (b) * * * (2)*** (ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days,	**§ 164.524 Access of individuals to protected health information.** * * * * * * * * * * (b) * * * (2)*** (ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request. (iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and (B) The covered entity may have only one such extension of time for action on a request for access.	Modified the subsection with provisions for providing access to PHI by individuals, PHI in a designated record set (and therefore EHRs as well), that is maintained in electronic form, if requested by the individual, must be provided to the individual in electronic form to the individual or another entity as directed by the individual. Also, modified the section relative to the costs that may be charged to the individual for such requests is limited to labor costs and media supplies only.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	provided that: (A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and (B) The covered entity may have only one such extension of time for action on a request for access. (c) * * * (2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. (iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if: (A) The individual agrees in advance to such a summary or explanation; and	(c) * * * (2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual. (ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if: (A) The individual agrees in advance to such a summary or explanation; and (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation. (3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. (4) * * * (i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual; * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation. (3) Time and manner of access. (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. (ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's 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. (4) * * * (i) Labor for copying the protected health information requested by the individual, 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; * * * * *			
56	In § 164.532, revise paragraphs (a), (c)(2), (c)(3), (d), (e)(1), and (e)(2), and add paragraphs (c)(4) and (f) to read as follows: **§ 164.532 Transition provisions.** (a) Standard: Effect of prior authorizations. Notwithstanding §§164.508 and 164.512(i), a	**§ 164.532 Transition provisions**. (a) *Standard: Effect of prior authorizations.* Notwithstanding §§164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal	Modified the subsection that requires business associate agreements to be executed that comply with all requirements of the HIPAA privacy and security rule as modified by the new HITECH provisions. Covered entities to business associates. Business associates	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i). * * * * * (c) * * * (2) The informed consent of the individual to participate in the research; (3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with §164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or (4) A waiver of authorization in accordance with § 164.512(i)(1)(i). (d) Standard: Effect of prior contracts or other arrangements with business associates. Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain or transmit protected health information on its behalf pursuant to a written contract or other written	permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB. * * * * * (c) * * * (2) The informed consent of the individual to participate in the research; or (3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with §164.508 if, after the compliance date, informed consent is sought from an individual participating in the research. (d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section. (e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this subpart,	to subcontractors. For business associate agreements that were executed prior to 1/25/2013 and are not set to terminate or renew before 9/23/2103, the time for compliance is the earlier of the renewal date or 9/22/2014, whichever occurs first. However, if any contracts are renewed or first executed after 1/25/2013, these must be conforming by 9/23/2013.	

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section. (e) Implementation specification: Deemed compliance. (1) Qualification. Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if: (i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and (ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013. (2) Limited deemed compliance period. A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of: (i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or (ii) September 22, 2014. * * * * * (f) Effect of prior data use agreements. If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e),	a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if: (i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and (ii) The contract or other arrangement is not renewed or modified from October 15, 2002, until the compliance date set forth in §164.534. (2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of: (i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in §164.534; or (ii) April 14, 2004. * * * * *		

	Final Rule Addition/Modification Text	Prior Version of Regulation	Explanation/Comments	Impact
	notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of: (1) The date such agreement is renewed or modified on or after September 23, 2013; or (2) September 22, 2014. * * * * *			