



Subpart A	General Provisions	
§ 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.	
§ 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.	
§ 160.103	Definitions.	
	Except as otherwise provided, the following definitions apply to this subchapter:	
	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 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. CMS stands for Centers	



	for Medicare & Medicaid Services within the Department of Health and Human Services. Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.	
	Covered entity means:	
(1)	A health plan.	
Subpart B	Preemption of State Law	
§ 160.201	Applicability.	
	The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.	
Subpart C	Compliance and Investigations Source: 71 FR 8424, Feb. 16, 2006, unless otherwise noted.	
§ 160.300	Applicability.	
Subpart D	Imposition of Civil Money Penalties	
§ 160.400	Applicability.	
	This subpart applies to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.	
§ 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.	
(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 §§164.314(a)(1)(ii) and 164.504(e)(1)(ii) of this subchapter, as applicable.	
Subpart E	Procedures for Hearings	
Subpart D	Standard Unique Health Identifier for Health Care Providers Source: 69 FR 3468, Jan. 23, 2004, unless otherwise noted	
§ 162.406	Standard unique health identifier for health care providers.	
§ 162.408	National Provider System.	
§ 162.410	Implementation specifications: Health care providers.	
(a)	A covered entity that is a covered health care provider must:	
(5)	If it uses one or more business associates to conduct standard transactions on its behalf, require its business associate(s) to use its NPI and other NPIs appropriately as required by the transactions that the business associate(s) conducts on its behalf.	



§ 162.412	Implementation specifications: Health plans.	
Subpart F	Standard Unique Employer Identifier Source: 67 FR 38020, May 31, 2002, unless otherwise noted	
[67 FR 38020, May 31, 2002, as amended at 69 FR 3469, Jan. 23, 2004]		



Subpart I	General Provisions for Transactions	
§ 162.920	Availability of implementation specifications.	
	<p>A person or an organization may directly request copies of the implementation standards described in subparts I through R of this part from the publishers listed in this section. The Director of the Office of the Federal Register approves the implementation specifications described in this section for incorporation by reference in subparts I through R of this part in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. The implementation specifications described in this paragraph are also available for inspection by the public at the Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, Maryland 21244 or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202-741-6030, or go to:</p> <p>http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html Copy requests must be accompanied by the name of the standard, number, if applicable, and version number. Implementation specifications are available for the following transactions:</p>	
(a)	General rule. Except as otherwise provided in this part, if a covered entity conducts with another covered entity (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard under this part, the covered entity must conduct the transaction as a standard transaction.	
(c)	Use of a business associate. A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:	
(1)	Comply with all applicable requirements of this part.	
(2)	Require any agent or subcontractor to comply with all applicable requirements of this part.	



PART 164	SECURITY AND PRIVACY	
Subpart C	Security Standards for the Protection of Electronic Protected Health Information	
§ 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. [65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]	
§ 164.104	Applicability.	
(a)	Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:	
(1)	A health plan.	
(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 of health care components of a covered entity.	
§ 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.	
(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 entities.	
(c)(1)	Standard: Documentation. A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.	
(2)	Implementation specification: Retention period. A covered entity must retain the documentation	



	as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	
--	---	--



Subpart C	Security Standards for the Protection of Electronic Protected Health Information Authority: 42 U.S.C. 1320d-2 and 1320d-4. Source: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.	
§ 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.	
§ 164.304	Definitions.	
§ 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.	
(2)	Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	
(3)	Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	
(4)	Ensure compliance with this subpart by its workforce.	
(b)	Flexibility of approach.	
(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.	
(iii)	The costs of security measures.	
(iv)	The probability and criticality of potential risks to electronic protected health information.	
(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)	Implementation specifications. In this subpart:	
(1)	Implementation specifications are required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.	
(2)	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 with reference to the likely contribution to protecting the entity's electronic protected health information; and	
(ii)	As applicable to the entity	
(A)	Implement the implementation specification if reasonable and appropriate; or	
(B)	If implementing the implementation specification is not reasonable and appropriate	
(1)	Document why it would not be reasonable and appropriate to implement the implementation specification; and,	
(2)	Implement an equivalent alternative measure if reasonable and appropriate.	
(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. [68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003]	
§ 164.308	Administrative safeguards.	
(a)	A covered entity must, in accordance with §164.306:	
(1)(i)	Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	
(ii)	Implementation specifications:	
(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.	
(B)	Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	
(C)	Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	
(D)	Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	
(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)	Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	
(ii)	Implementation specifications:	
(A)	Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	
(B)	Workforce clearance procedure (Addressable). Implement procedures to determine that the	



	access of a workforce member to electronic protected health information is appropriate.	
(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)	Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	
(ii)	Implementation specifications:	
(A)	Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	
(B)	Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	
(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.	
(5)(i)	Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).	
(ii)	Implementation specifications. Implement:	
(A)	Security reminders (Addressable). Periodic security updates.	
(B)	Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	
(C)	Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	
(D)	Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	
(6)(i)	Standard: Security incident procedures. Implement policies and procedures to address security incidents.	
(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 security incidents and their outcomes.	
(7)(i)	Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	
(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.	
(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).	
§ 164.310	Physical safeguards.	
	A covered entity must, in accordance with §164.306: (a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	
(2)	Implementation specifications:	
(i)	Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency	
(ii)	Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	
(iii)	Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	
(iv)	Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	
(b)	Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	
(c)	Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	
(d)(1)	Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	
(2)	Implementation specifications:	
(i)	Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	



(ii)	Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	
(iii)	Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	
(iv)	Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	
§ 164.312	Technical safeguards.	
	A covered entity must, in accordance with §164.306: (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	
(2)	Implementation specifications:	
(i)	Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.	
(ii)	Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	
(iii)	Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	
(iv)	Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	
(b)	Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	
(c)(1)	Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	
(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	
(d)	Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	
(e)(1)	Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	
(2)	Implementation specifications:	
(i)	Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
(ii)	Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	
§ 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 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 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)(1)	Standard: Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	
(2)	Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—	
(i)	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 group health plan;	
(ii)	Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	
(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	
(iv)	Report to the group health plan any security incident of which it becomes aware.	
§ 164.316	Policies and procedures and documentation requirements.	
	A covered entity must, in accordance with §164.306:	
(a)	Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. 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.	
(b)(1)	Standard: Documentation.	
(i)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	
(ii)	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	
(2)	Implementations:	
	(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	
	(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	
	(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health	



	information.	
--	--------------	--



Subpart E	Privacy of Individually Identifiable Health Information	
§ 164.500	Applicability.	
(a)	Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.	
§ 164.501	Definitions.	
	As used in this subpart, the following terms have the following meanings:	
	Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.	
§ 164.502	Uses and disclosures of protected health information: general rules	
(d)	Standard: Uses and disclosures of de-identified protected health information.	
(1)	Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.	
(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 §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.	
(g)(1)	Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.	
(j)	Standard: Disclosures by whistleblowers and workforce member crime victims	
(1)	Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:	
(i)	The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and	
(ii)	The disclosure is to:	
(A)	A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or	
(B)	An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.	
(1)	That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and	
(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	
(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; 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 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 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.	
(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 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.	
(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 the confidentiality of the information has been breached.	
§ 164.514	Other requirements relating to uses and disclosures of protected health information.	



(d)(1)	Standard: Minimum necessary requirements. In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.	
(3)	Implementation specification: Minimum necessary disclosures of protected health information.	
(C)	The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or	
(e)(1)	Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.	
(3)	Implementation specification: Permitted purposes for uses and disclosures.	
(ii)	A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose , whether or not the limited data set is to be used by the covered entity.	
(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:	



§ 164.526	Amendment of protected health information.	
(a)	Standard: Right to amend.	
(b)	Implementation specifications: Requests for amendment and timely action.	
(1)	Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment , provided that it informs individuals in advance of such requirements.	
(2)	Timely action by the covered entity.	
(i)	The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.	
(A)	If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.	
(B)	If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.	
(ii)	If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days , provided that:	
(A)	The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, 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 an amendment.	
(c)	Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.	
(1)	Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by , at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.	
(2)	Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.	
(3)	Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:	
(i)	Persons identified by the individual as having received protected health information about the individual and needing the amendment; and	
(ii)	Persons, including business associates , that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied , or could foreseeably	



	rely, on such information to the detriment of the individual.	
--	--	--



§ 164.528	Accounting of disclosures of protected health information.	
(a)	Standard: Right to an accounting of disclosures of protected health information.	
(1)	An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:	
(i)	To carry out treatment, payment and health care operations as provided in §164.506;	
(ii)	To individuals of protected health information about them as provided in §164.502;	
(iii)	Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502;	
(iv)	Pursuant to an authorization as provided in §164.508;	
(v)	For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510;	
(vi)	For national security or intelligence purposes as provided in §164.512(k)(2);	
(vii)	To correctional institutions or law enforcement officials as provided in §164.512(k)(5);	
(viii)	As part of a limited data set in accordance with §164.514(e); or	
(ix)	That occurred prior to the compliance date for the covered entity.	
(2)(i)	The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in §164.512(d) or (f) respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.	
(ii)	If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:	
(A)	Document the statement , including the identity of the agency or official making the statement;	
(B)	Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and	
(C)	Limit the temporary suspension to no longer than 30 days from the date of the oral statement , unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.	
(3)	An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.	
(b)	Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.	
(1)	Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.	
(2)	Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must	



	include for each disclosure:	
(i)	The date of the disclosure;	
(ii)	The name of the entity or person who received the protected health information and, if known, the address of such entity or person;	
(iii)	A brief description of the protected health information disclosed ; and	
(iv)	A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§164.502(a)(2)(ii) or 164.512, if any.	
(3)	If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:	
(i)	The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;	
(ii)	The frequency, periodicity, or number of the disclosures made during the accounting period; and	
(iii)	The date of the last such disclosure during the accounting period.	
(4)(i)	If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with §164.512(i) for 50 or more individuals , the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:	
(A)	The name of the protocol or other research activity ;	
(B)	A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;	
(C)	A brief description of the type of protected health information that was disclosed;	
(D)	The date or period of time during which such disclosures occurred , or may have occurred, including the date of the last such disclosure during the accounting period;	
(E)	The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and	
(F)	A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.	
(ii)	If the covered entity provides an accounting for research disclosures , in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.	
(c)	Implementation specifications: Provision of the accounting.	
(1)	The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.	
(i)	The covered entity must provide the individual with the accounting requested ; or	



(ii)	If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days , provided that:	
(A)	The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting ; and	
(B)	The covered entity may have only one such extension of time for action on a request for an accounting.	
(2)	The covered entity must provide the first accounting to an individual in any 12 month period without charge . The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.	
(d)	Implementation specification: Documentation . A covered entity must document the following and retain the documentation as required by §164.530(j):	
(1)	The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;	
(2)	The written accounting that is provided to the individual under this section; and	
(3)	The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.	



§ 164.530	Administrative requirements.	
(a)(1)	Standard: Personnel designations.	
(i)	A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.	
(ii)	A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.	
(2)	Implementation specification: Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.	
(b)(1)	Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.	
(2)	Implementation specifications: Training.	
(i)	A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:	
(A)	To each member of the covered entity's workforce by no later than the compliance date for the covered entity;	
(B)	Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and	
(C)	To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.	
(ii)	A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.	
(c)(1)	Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.	
(2)(i)	Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.	
(ii)	A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.	
(d)(1)	Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.	
(2)	Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.	



(e)(1)	Standard: Sanctions . A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of §164.502(j) or paragraph (g)(2) of this section.	
(2)	Implementation specification: Documentation . As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.	
(f)	Standard: Mitigation . A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.	