

HIPAA Security Rule Policy Map

Document Information	
Identifier	
Status	Published
Published	02/15/2008
Last Reviewed	02/15/1008
Last Updated	02/15/2008
Version	1.0

Revision History

Version	Published	Author	Description
1.0	02/15/2008	Doug Markiewicz	Initial publication.

HIPAA Security Rule Policy Map

The following provides a mapping of the University's Health Insurance Portability and Accountability Act ("HIPAA") Information Security Policy to the HIPAA Security Rule defined in the Code of Federal Regulations, 45 C.F.R. 164.

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Standard	X	05 – 22
164.308(a)(1)(ii)(A)	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.	Implementation Specification (Required)		05b
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Implementation Specification (Required)		05c
164.308(a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures for the covered entity.	Implementation Specification (Required)		Enforcement
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Implementation Specification (Required)		
164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Standard		01
164.308(a)(3)(i)	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.	Standard	X	07 - 09, 17, 18
164.308(a)(3)(ii)(A)	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.	Implementation Specification (Addressable)		
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Implementation Specification (Addressable)		
164.308(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information	Implementation Specification		

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
	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.	(Addressable)		
164.308(a)(4)(i)	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.	Standard	X	07
164.308(a)(4)(ii)(A)	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.	Implementation Specification (Required)	X	07 - 09
164.308(a)(4)(ii)(B)	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.	Implementation Specification (Addressable)	X	07 – 09
164.308(a)(4)(ii)(C)	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.	Implementation Specification (Addressable)	X	07
164.308(a)(5)(i)	Implement security awareness and training program for all members of its workforce (including management).	Standard		14
164.308(a)(5)(ii)(A)	Periodic security updates.	Implementation Specification (Addressable)		
164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.	Implementation Specification (Addressable)		
164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.	Implementation Specification (Addressable)		
164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.	Implementation Specification (Addressable)		
164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	Standard	X	15 – 16
164.308(a)(6)(ii)(A)	Identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to the covered entity; and document security incidents and their	Implementation Specification (Required)		15 – 16

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
	outcomes.			
164.308(a)(7)(i)	Establish 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.	Standard	X	10c
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Implementation Specification (Required)		
164.308(a)(7)(ii)(B)	Establish procedures to restore any loss of data.	Implementation Specification (Required)		
164.308(a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Implementation Specification (Required)		
164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.	Implementation Specification (Addressable)		
164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Implementation Specification (Addressable)		05b, 10c
164.308(a)(8)	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.	Standard		05b
164.308(b)(1) 164.314(a)	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. NOTE: See Security Rule for exceptions. Additional provisions documented in 164.314.	Standard		06
164.308(b)(4)	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associated that meets the applicable requirements of	Implementation Specification (Required)		06

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
	164.314(a).			
164.310(a)(1)	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.	Standard	X	17 - 22
164.310(a)(2)(i)	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.	Implementation Specification (Addressable)		
164.310(a)(2)(i)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Implementation Specification (Addressable)	X	17 - 22
164.310(a)(2)(iii)	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.	Implementation Specification (Addressable)		
164.310(a)(2)(iv)	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).	Implementation Specification (Addressable)	X	19
164.310(b)	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.	Standard	X	07b, 07c, 08, 09, 11 and 18 Also see CMU Computing Policy
164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Standard		09, 17 and 18
164.310(d)(1)	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.	Standard	X	10a, 17, 18 20 and 21
164.310(d)(2)(i)	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.	Implementation Specification (Required)	X	20
164.310(d)(2)(ii)	Implement procedures for removal of electronic protected health information from	Implementation Specification		

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
	electronic media before the media are made available for re-use.	(Required)		
164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Implementation Specification (Addressable)		21
164.310(d)(2)(iv)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Implementation Specification (Addressable)		
164.312(a)(1)	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).	Standard	X	05c, 07 – 09, 12 and 13
164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	Implementation Specification (Required)		
164.312(a)(2)(ii)	Establish procedures for obtaining necessary electronic protected health information during an emergency.	Implementation Specification (Required)		
164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Implementation Specification (Addressable)		
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	Implementation Specification (Addressable)		12 and 13
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Standard		
164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Standard	X	05c, 07 – 09, 12 and 13
164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in any unauthorized manner.	Implementation Specification (Addressable)		
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Standard		
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Standard		12

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Implementation Specification (Addressable)		05c, 07 – 09, 12 and 13
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Implementation Specification (Addressable)		12 and 13
164.314(b)(1)	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 related, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Standard		
164.314(b)(2)	The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to <ul style="list-style-type: none"> (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that is creates, received, maintained, 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 to protect the information (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 (iv) Report to the group health plan any security incident of which it becomes aware 	Implementation Specification (Required)		
164.316(a)	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	Standard	X	All

HIPAA Security Rule Reference	Requirement	Type	Policy Required	CMU's HIPAA Policy Ref.
	procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.			
164.316(b)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form. If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of that action, activity, or assessment.	Standard		All
164.316(b)(i)	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.	Implementation Specification (Required)		Maintenance
164.316(b)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Implementation Specification (Required)		
164.316(b)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Implementation Specification (Required)		Maintenance