Health Information Technology for Economic and Clinical Health (HITECH) Act
Cross-walk between current Business Associate Agreement and new HITECH Act requirements
Effective February 17, 2010

Prepared by the
Security Compliance for Business Associates Subcommittee
of the
ABA Health Law Section HITECH Task Force

November 12, 2009

Security Compliance for Business Associates Subcommittee Membership

S. Christopher Byers
PNC Treasury Management
(412) 762-4654
s.byers@pnc.com

Keith Cheresko
2840 Rae Lynn
Milford, MI 48381
(248) 684-6741
keith@cheresko.net

Craig A. Clesson
King Pharmaceuticals
501 Fifth Street
Bristol, TN 37620
(800) 776-3637
Craig.Clesson@kingpharm.com

Sheila Deselich Cohen
1657 Wingate Drive
Delaware, Ohio 43015
(740) 917-5155
sdcohen@columbus.rr.com

David Ermer
Ermer & Brownell, PLLC
1828 L St., NW, Suite 640
Washington, DC 20036
(202) 833-3400 ext. 1009
dermer@ermerlaw.com

Will Hughes
ADAMS & GRAHAM, L.L.P.
134 East Van Buren, Suite 301
Harlingen, Texas 78550
phone: (956) 428-7495
willhughes@adamsgraham.com

Lee Kim
Tucker Arensberg, P.C.
1500 One PPG Place
Pittsburgh, PA 15222
412-594-3915
lkim@tuckerlaw.com

Tracy Vigness Kolb
ZUGER KIRMIS & SMITH
PO Box 1695
316 North Fifth Street
Bismarck, ND 58502-1695
(701) 223-2711
tkolb@zkslaw.com

Kevin M. Kramer
Gibbons PC
One Gateway Center
Newark, NJ 07102-5310
973-596-4651
kkramer@gibbonslaw.com

Linda R. Mendel
Vorys, Sater, Seymour and Pease LLP
52 East Gay St
Columbus, Ohio 43215
(614) 464-8218
lrmendel@vorys.com

Brad M Rostolsky
Reed SmithLLP
2500 One Liberty Place
1650 Market St
Philadelphia, PA 19103
(215) 851-8195
brostolsky@reedsmith.com

Marty Rowan
Law Office of Marcia A. Rowan, PLLC
1213 Culbreth Dr
Wilmington, NC 28405
(910) 256-7947
marty@rowanlawfirm.com

Robert H. Schwartz
Butzel Long
Stoneridge West
41000 Woodward Ave.
Bloomfield Hills, MI 48304
(248) 258-2611
schwartzrh@butzel.com

This Committee is part of the ABA's HITECH Act Task Force

Task Force Chairman

John R. Christiansen
Christiansen IT Law
206.301.9412
john@christiansenlaw.net

ABA Liaison

Simeon Carson
Membership, Technology & Publication Specialist
ABA Health Law Section
321 N. Clark St.
Chicago, IL 60654-7598
(312) 988-5824
carsons@staff.abanet.org

Introduction

The HITECH Act directly applies the administrative, physical, and technical safeguard requirements of the HIPAA Security Rule, 45 C.F.R Parts 160 and 164, Subparts A and C, to business associates ("BA") of covered entities ("CE"), effective February 17, 2010. This document cross-walks business associates from the relevant provisions of the current business associate agreement to the pertinent statutorily mandated safeguards.

Scope of the Security Rule

The Security Rule applies to electronic protected health information ("EPHI"). EPHI is Individually Identifiable Health Information as defined at 45 C.F.R. § 160.103 that a CE or BA stores in electronic media or transmits by electronic media, subject to the exceptions for certain educational records and employment records. Consequently, it makes sense to focus on the key definition of "electronic media." The Security Rule applies to PHI that is stored internally or externally in

> 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

and to PHI internally or externally transmitted by electronic media, meaning

> 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.

45 C.F.R. § 160.103. See also Preamble, at 8,338[1] (The Security Rule "draws no distinction between internal and external data movement.") Although the HIPAA Transaction and Code Set standards apply only to transactions between CEs, the Security Rule applies to all EPHI transmissions made by a CE or a BA, including, for example, those made to plan members or patients. See id. The Preamble further clarifies that the Security Rule applies to devices that provide input or output to the organization's computers, such as interactive voice response or fax-back services. In such cases, the Security Rule generally does not apply to the incoming telephonic transmission.

[1] All Preamble references in this cross-walk are to the Department of Health and Human Services regulatory preamble to the Final Security Rule, published at 68 Fed. Reg. 8,334 on February 20, 2003. The Preamble assumes application of the Security Rule to HIPAA Covered Entities. Readers of this cross-walk should interpret the Preamble's Covered Entity references to extend to Business Associates.

but it does apply to the outgoing computer-based transmission. Id. HHS also provides in the Preamble a significant interpretation of the term “computer” which is used in the defined term “electronic media,” quoted above. This interpretation limits the scope of the Security Rule. According to the Preamble (68 Fed. Reg. at 8,342),

> Although most recently made electronic devices contain microprocessors (a form of computer) controlled by firmware (an unchangeable form of computer program), we intend the term "computer" to include only software programmable computers, for example, personal computers, minicomputers, and mainframes. Copy machines, fax machines, and telephones, even those that contain memory and can produce multiple copies for multiple people are not intended to be included in the term "computer." Therefore, because "paper-to-paper" faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this [Security] rule. [However those activities are covered by the Privacy Rule.]

(Emphasis added.) In sum, the Security Rule’s EPHI definition reaches a broad range of activities from storing massive amounts of data on claims processing systems to a simple Microsoft EXCEL spreadsheet containing PHI that is stored on a desktop computer, and from transmitting of PHI between sophisticated business associates to e-mails or instant messages with consumers. HHS’s “computer” definition places a clear limit on the Security Rule’s scope.

Structure of the Security Rule

As reflected in the cross-walk, the Safeguards are comprised of required security standards. Most standards include implementation specifications, which describe methods or ways of achieving compliance with the standards (see 45 C.F.R. § 164.306(d)). Where there are no implementation specifications corresponding to particular standards, “the standards themselves serve as the implementation specification.” Preamble, at 8,336. HHS explained that it listed the standards, and within the standards the implementation specifications, in a "logical" order that reflects their importance in the larger scheme of security compliance (id., at 8,344). The cross walk generally follow this order.

As reflected in the cross walk, the Security Standards include both required and addressable implementation specifications. According to HHS (Preamble, at 8,334), the thirteen required implementation specifications are "generally accepted industry practices" and were drawn from the sixth chapter of the National Research Council’s 1997 report titled “For the Record: Protecting Electronic Health Information.”

A CE or BA must examine the Security Rule's addressable implementation specifications its own security environment, and managers must determine whether to implement them or, in some cases, alternative measures that also meet the specification's goal. The Preamble (at 8,336) explains that "The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation."[2] According to HHS (id.), if the analysis leads to the conclusion that "a given addressable implementation specification is reasonable and appropriate, the covered entity must implement it." However, if the analysis leads to the conclusion that "a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification." Id. HHS warns that "an entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard." Id.

The Security Rule, 45 CFR § 164.306(d), and the Preamble further note that no action may be necessary in some cases. "A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification" (Preamble, at 8,345). "In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met." Id.

[2] The Security Rule, 45 C.F.R. § 164.306(d), states that:

> When a standard.* * *.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.

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

Current Business Associate Contract Obligation	**HITECH Act Obligation (Sec. 13401(a) quoted to the right) – effective 2/17/2010**	"Section 164.308 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity."	
	Security Standard	*Implementation Specifications*	*Explanation*
BA agrees to use appropriate **administrative** * * * safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI it creates, receives, maintains or transmits on behalf of the CE to prevent unauthorized use or disclosure of such EPHI. 45 C.F.R. § 164.314(a)(2)(i)(A).	Security Management Process 45 C.F.R. § 164.308(a)(i)(1) "Implement policies and procedures to prevent, detect, contain, and correct security violations." This risk standard and its implementation specifications are the "foundation upon which an entity's security activities are built" (Preamble at 8,346). Entities must "periodically" conduct a risk analysis re-assessment and update its risk analysis as needed.	Risk Analysis (Required) 45 C.F.R. § 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 EPHI held by the covered entity." This risk analysis should attempt to disclose "all relevant losses" that could be anticipated if security measures were not in place, such as "losses caused by inappropriate uses and disclosures and the loss of data integrity that would occur absent the security measures." Preamble, at 8,347,
		Risk Management (Required) 45 C.F.R. § 164.308(a)(1)(ii) B)	**"**Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [45 C.F.R. §] 164.306(a)."
		Sanction Policy (Required) 45 C.F.R. § 164.308(a)(1)(ii)(C)	**"**Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the [organization]." The details of this policy, such as types of sanctions and instances in which they will be applied, are left up to the organization (Preamble, at 8,348). Sanctions will be based on "the relative severity of the violation" and on the entity's own security policies. Id.

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

	Security Standard	Implementation Specifications	Explanation
		Information System Activity Review (Required) 45 C.F.R. § 164.308(a)(1)(ii)(D)	"Implement procedures to regularly audit and review records of information system activity, such as audit logs, access reports, and security incident tracking reports." The Security Rule. 45 C.F.R. § 164.304, defines "information systems" as "an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."
	Assigned Security Responsibility 45 C.F.R. § 164.308(a)(2)	No implementation specifications for this standard	"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity." Entities may appoint more than one person with security duties but the Preamble, at 8,347, is clear that a single person must be assigned "overall final responsibility" for security. The person appointed must understand HIPAA laws and regulations; establish appropriate levels of oversight; support education, awareness and hotline reporting activities; conduct periodic HIPAA risk assessments; participate in the development of corrective action plans and mitigation strategies for identified security risks; and track progress and ensure risks are appropriately communicated to senior management and board. Id.
	Workforce Security 45 C.F.R. § 164.308(a)(3)(i) "Implement policies and procedures to ensure that all workforce members have appropriate access to EPHI, as provided Information Access Standard, and to prevent those workforce members who do not have access from obtaining access to EPHI."	Authorization and/or Supervision (Addressable) 45 C.F.R. § 164.308(a)(3)(ii)(A)	"Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where EPHI might be accessed," such as maintenance personnel. As an addressable specification, "entities can decide on the feasibility of meeting this specification based on their risk analysis" (Preamble, at 8,348). *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 entity. 45 C.F.R. § 160.103

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

	Security Standard	Implementation Specifications	Explanation
		Workforce Clearance Procedure (Addressable) 45 C.F.R. § 164.308(a)(3)(ii)(B)	"Implement procedures to determine that the access of a workforce member to EPHI is appropriate." Prevent unauthorized workforce members from obtaining access to EPHI. HHS expects "effective personnel screening processes" from entities whose risk analysis indicates this is necessary. The extent of such screening will be based on an assessment of "risk, cost, benefit, and feasibility as well as other protective measures in place." Preamble, at 8,348. It is clear from the Preamble, id., that HHS only intends the smallest of covered entities to exempt themselves from this addressable implementation specification.
		Termination Procedures (Addressable) 45 C.F.R. § 164.308(a)(3)(ii)(C)	"Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made as specified in [workforce clearance procedures]". The purpose of this specification is to ensure that security-related issues are addressed when a colleague is terminated or when a colleague's EPHI access is revoked under the workforce clearance procedures. Entities can show this is being done by revoking passwords, "changing combination locks, removal from access lists, removal of user account(s), and the turning in of keys, tokens, or cards that allow access." Further, workforce access needs to be appropriate based on job duties. An audit mechanism should be in place that identifies who accesses data. (Preamble, at 8,348).
	Information Access Management 45 C.F.R. § 164.308(a)(4)(i) "Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of [the Privacy Rule]."	Isolate Healthcare Clearing House Functions (Required) 45 C.F.R. § 164.308(a)(4)(ii)(A)	If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization. Healthcare and clearing house functions within a single organization must be separated.
		Access Authorization (Addressable) 45 C.F.R. § 164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism." Implement policies and procedures to address how workstations, transactions, programs where EPHI resides are accessed by users. The Security Rule, 45 C.F.R. § 164.304, defines "workstation" as "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, [such as a personal digital assistant] and electronic media stored in its immediate environment."

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

	Security Standard	Implementation Specifications	Explanation
		Access Establishment and Modification (Addressable) 45 C.F.R. § 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." Periodic service and documentation of user permission for rights of access to a workstation, transaction, program or process should be undertaken.
	Security Awareness and Training 45 C.F.R. § 164.308(a)(5)(i) "Implement a security awareness and training program for all members of its workforce (including management)." HHS describes training as a "critical activity." Entities are required to initially train their workforce "as reasonable and appropriate to carry out their functions at the facility" before the compliance date. "Training should be an on-going, evolving process in response to environmental and operational changes affecting the security of EPHI. Each entity must determine the appropriate amount and type of training, based on its "configuration and security risks." Preamble at 8,349-50	Security Reminders (Addressable) 45 C.F.R. § 164.308(a)(5)(ii)(A)	Provide periodic security updates to the workforce. Create screensavers, posters, in-service training and communications to ensure that all employees understand their role in securing EPHI.
		Protection from Malicious Software (Addressable) 45 C.F.R. § 164.308(a)(5)(ii)(B)	"Implement procedures for guarding against, detecting, and reporting malicious software." "Malicious software means software, for example, a virus, designed to damage or disrupt a system." 45 C.F.R § 164.304. Policies and procedures to evaluate new software, protect bootable drives, corporate anti-virus procedures, firewalls and intrusion detection. Id. § 164.308(a)(5)(ii)(B)

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

	Security Standard	Implementation Specifications	Explanation
		Log-in Monitoring (Addressable) 45 C.F.R. § 164.308(a)(5)(ii)(C)	"Implement procedures for monitoring log-in attempts and reporting discrepancies."
		Password Management (Addressable) 45 C.F.R. § 164.308(a)(5)(ii)(C)	**"**Implement procedures for creating, changing, and safeguarding passwords." Password means confidential authentication information composed of a string of characters. 45 C.F.R. §§ 164.304
	Contingency Plan 45 C.F.R. § 164.308(a)(7)(i) "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 EPHI."	Data Backup Plan (Required) 45 C.F.R. §§ 164.308(a)(7)(ii)(A)	"Establish and implement procedures to create and maintain retrievable exact copies of EPHI." According to the Preamble, at 8,354, "the data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan should define exactly what information is needed to be retrievable to allow the entity to continue business 'as usual' in the face of damage or destruction of data, hardware, or software. For example, "the extent to which e-mail backup would be needed would be determined through that analysis." Provide for procedures to create and maintain retrievable exact copies of EPHI.
		Disaster Recovery Plan (Required) 45 C.F.R. §§ 164.308(a)(7)(ii)(B)	"Establish (and implement as needed) procedures to restore any loss of data." Entities are required to predict how "natural disasters" could affect systems that contain EPHI and how it will respond to such events. Implement policies and procedures to restore data from backup media, including operating systems, subsystems, utilities and applications.
		Emergency Mode Operation Plan (Required) 45 C.F.R. §§ 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 EPHI while operating in emergency mode." The Preamble, at 8,351, clarifies that it is only necessary to operate "those critical business processes that must occur to protect the security of EPHI during and immediately after a crisis situation."
		Testing and Revision Procedure (Addressable) 45 C.F.R. §§ 164.308(a)(7)(ii)(D)	"Implement procedures for periodic testing and revision of contingency plans. Entities will need to determine, based on size, configuration, and security environment, how much of the plan to test and/or revise."

ADMINISTRATIVE SAFEGUARDS

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. 45 C.F.R § 164.304

	Security Standard	Implementation Specifications	Explanation
		Applications and Data Criticality Analysis (Addressable) 45 C.F.R. §§ 164.308(a)(7)(ii)(E)	“Assess the relative criticality of specific applications and data in support of other contingency plan components.” 45 C.F.R. §§ 164.308(a)(7)(ii)(E)
	Evaluation 45 C.F.R. § 164.308(a)(8)(i)	No implementation specifications for this standard	“Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI that establishes the extent to which an entity's security policies and procedures meet the [Security Rule’s] requirements.” This standard is inextricably intertwined with the risk assessment and management implementation specifications. The Evaluation standard requires entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity’s security policy and the Security Rule. It is important to note that this evaluation is to include technical and non-technical components of security, which presumably would activities such as training. Knowledge of new threats or risks, as well as new technology, can also prompt a new evaluation. Preamble, at 8,351-52.

PHYSICAL SAFEGUARDS

Physical safeguards are “physical measures, policies, and procedures to protect a CEs electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.” 45 C.F.R. § 164.304

Current Business Associate Contract Obligation	**HITECH Act Obligation (Sec. 13401(a) quoted to the right) – effective 2/17/2010**	“Section 164.310 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity.”	
	Security Standard	*Implementation Specifications*	*Explanation*
BA agrees to use appropriate **physical** * * * safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI it creates, receives, maintains or transmits on behalf of the Covered Entity to prevent unauthorized use or disclosure of such EPHI. 45 C.F.R. § 164.314(a)(2)(i)(A).	Facility Access Controls 45 C.F.R. § 164.310(a)(1)(i) “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.” The term “facility” means “the physical premises and the interior and exterior of a building(s).” 45 C.F.R. § 164.304	Contingency Operations (Addressable) 45 C.F.R. §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.”
		Facility Security Plan (Addressable) 45 C.F.R. §164.310(a)(2)(ii).	“Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.”
		Access Control & Validation Procedure (Addressable) 45 C.F.R. §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.”
		Maintenance Records (Addressable) 45 C.F.R. §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).”
	Workstation Use 45 C.F.R. § 164.310(b)	No implementation specifications for this standard	“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 EPHI.” A workstation is defined as "an electronic computing device [such as] a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment." 45 C.F.R. § 164.304.

PHYSICAL SAFEGUARDS

Physical safeguards are “physical measures, policies, and procedures to protect a CEs electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.” 45 C.F.R. § 164.304

	Security Standard	Implementation Specifications	Explanation
	Workstation Security 45 C.F.R. § 164.310(c)	No implementation specifications for this standard	“Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users.” Each organization must adopt physical safeguards to restrict access to information available through a workstation, as defined in 45 C.F.R. § 164.304.
	Device and Media Controls 45 C.F.R. § 164.310(d)(1) **“**Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.”	Disposal (Required) 45 C.F.R. § 164.310(d)(2)(i)	“Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.”
		Media Re-use (Required) 45 C.F.R. § 164.310(d)(2)(ii)	“Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.” Electronic media, of course, is broadly defined to include such easily portable items as CD-ROMs, floppy disks, and zip drives.
		Accountability (Addressable) 45 C.F.R. § 164.310(d)(2)(iii)	“Maintain a record of the movements of hardware and electronic media and any person responsible therefore.” This specification requires organizations to keep a record of equipment assigned to an individual as it moves in or out of a facility. This could be as simple as a receipt for returned or signed out equipment, recorded in a log, and is not expected to be a costly or terribly elaborate process. According to HHS, “maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services" (Preamble, at 8,353)
		Data Backup and Storage (Addressable) 45 C.F.R. § 164.310(d)(2)(iv)	“Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.” This specification is narrow in scope and concerns creating a back-up of only that data an entity might need to retrieve to allow business to continue in the event of damage or destruction of "data, hardware or software."

Current Business Associate Contract Obligation	**HITECH Act Obligation (Sec. 13401(a) quoted to the right) – effective 2/17/2010**	Section 164.312 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity.	
	Security Standard	*Implementation Specifications*	*Explanation*
BA agrees to use appropriate * * * **technical** safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI it creates, receives, maintains or transmits on behalf of the CE to prevent unauthorized use or disclosure of such EPHI. 45 C.F.R. § 164.314(a)(2)(i)(A)	Access Control 45 C.F.R. § 312(a)(1) **"**Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."	Unique User Identification (Required) 45 C.F.R. § 312(a)(2)(i)	"Assign a unique name and/or number for identifying and tracking user identity. Log user activity for that particular user. Implement effective access controls. EPHI should be kept secure from unauthorized access. EPHI may be encrypted to ensure security."[3]
	Emergency Access Procedure 45 C.F.R. § 146.312(a)(2)(ii) "Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency."	Emergency Access Procedure (Required) 45 C.F.R. § 312(a)(2)(ii)	"Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency." Information systems must have a mechanism for providing a bypass predefined access controls to allow access to EPHI during an emergency; however, at the same time, access controls should be in place to ensure that emergency procedures are not used to obtain unauthorized access or access control rights.[4] HHS appears to understand that such access will not always be achievable. The Preamble, at 8,355, suggests that procedures will serve to "provide guidance on possible ways to gain access" in instances when "normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster."

[3] Stephen S. Wu, ed., A Guide to HIPAA Security and the Law, 78 (ABA 2007).

[4] *Id.* at 79.

TECHNICAL SAFEGUARDS

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304

	Security Standard	*Implementation Specifications*	*Explanation*
	Automatic Log-Off 45 C.F.R. §164.312(a)(2)(iii) "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."	Automatic Logoff (Addressable) 45 C.F.R. § 312(a)(2)(iii)	"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity." Security risks to be managed include logged-in users that leave their workstations unattended. The technical safeguard would either terminate or suspend their session after a predetermined amount of time has passed due to inactivity.[5]
	Encryption and Decryption 45 C.F.R. §164.312(a)(2)(iv) "Implement a mechanism to encrypt and decrypt EPHI."	Encryption and Decryption (Addressable) 45 C.F.R. § 312(a)(2)(iv)	"Implement a mechanism to encrypt and decrypt EPHI." The Security Rule, 45 C.F.R. § 164.304, defines "encryption" as use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." According to the Preamble, at 8,355, "the use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule." In other words, EPHI residing on storage media such as disks, tapes, CD-ROMs, etc. must be encrypted if reasonable and appropriate. If the security risks of storing data in the "clear" (i.e., unencrypted) or otherwise transmitting data in the "clear" is unacceptably high and if no equivalent alternative security measures would provide commensurate security, then the EPHI must be encrypted. Documentation of the reasoning regarding the security measures must be made regardless of whether encryption is used or equivalent alternative measures.[6]

[5] *Id.* at 80.

[6] *Id.* at 80. The HHS Interim Rule on Breach Notification for Unsecured Protected Health Information published at 74 Fed. Reg. 42,740 (August 24, 2009) highlights the current importance of encrypting EPHI.

TECHNICAL SAFEGUARDS

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304

	Security Standard	*Implementation Specifications*	*Explanation*
	Audit Controls 45 C.F.R. § 312(b)	No implementation specifications for this standard,	"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI." ." The technical safeguard must be a technical method for logging user activity and a method, automated or procedural, for examining that activity log for unauthorized activity.[7] According to the Preamble, at 8,355, "entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses," including "how intensive any audit control function should be." HHS directs entities to guidance found in NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security.
	Integrity 45 C.F.R. § 312(c)(1) "Implement policies and procedures to protect EPHI from improper alteration or destruction." HHS believes (Preamble, at 8,356) that "this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task."	Mechanism to Authenticate EPHI (Addressable) 45 C.F.R. § 312(c)(2)	"Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner." The Preamble, at 8,356, cites "error correcting memory and magnetic disc storage" as to ways to verify or authenticate the integrity of the data." EPHI should not be corrupted or otherwise tampered with. EPHI may be digitally signed to provide strong assurance of security. However, an unverified digital signature may indicate that the EPHI has been corrupted or otherwise has been tampered with. In addition, the sender and receiver of the EPHI may verify that the data has not been tampered with by making sure that the checksum generated from the EPHI is the same, presuming that the sender and the receiver of the EPHI use the same method for calculating the checksum. Soft tokens may also be used for EPHI integrity verification.[8]

[7] *Id.* at 81.
[8] *Id.* at 82-83.

TECHNICAL SAFEGUARDS

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304

	Security Standard	*Implementation Specifications*	*Explanation*
	Person or Entity Authentication 45 C.F.R. § 312(d)	No implementation specifications for this standard	"Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed." The Preamble, at 8,356, describes this standard as a general requirement that might be met with little difficulty, given the common features of digital signatures and soft tokens. The technical safeguard should enforce access control policies and procedures via authentication to ensure that a person seeking to log on to a system is the authorized user he or she purports to be.[9] Authentication mechanisms include the following: 1) Password or PIN;* 2) Magnet swipe card, smart card, or other physical token; 3) Biometric identifiers (e.g., fingerprints, iris patterns, voice patterns, etc.); 4) Digital signatures; 5) Digital certificates; and 6) Public/private key pairings.[10] Strong passwords or PIN's should be chosen by the user (e.g., the use of non-alphanumeric symbols or non-dictionary words). The user must also be instructed on whom to notify in case a password or PIN is compromised.[11]

[9] *Id.* at 83.
[10] *Id.* at 83-85.
[11] *Id.* at 85.

TECHNICAL SAFEGUARDS

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304

	Security Standard	*Implementation Specifications*	*Explanation*
	Transmission Security 45 C.F.R. § 312(e)(1) “Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.”	Integrity Controls (Addressable) 45 C.F.R. § 312(e)(2)(i)	“Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.” Security threats to internal networks or a network such as the Internet include the following: 1) Packet sniffing (also known as eavesdropping[12]) wherein an unauthorized person captures unprotected EPHI over a network; and 2) Data modification: interception and modification of EPHI by an unauthorized person in a way that the recipient cannot detect;[13] and 3) Key logging (another form of eavesdropping) where an unauthorized person captures unprotected EPHI either by logging the activity on the user’s local machine or over a network. The technical safeguard should include a method for secure transmission of EPHI such as using a virtual private network (“VPN”) or secure sockets layer (“SSL”)[14] connection. In addition, public/private keys, digital signatures, and/or checksums may be used to verify that data has not been tampered with. Steps should also be taken to ensure that there are no spyware, malware, or other malicious programs that may log user activity and transmissions such as of EPHI, either on the user’s workstation or the server. Implement a mechanism to encrypt EPHI whenever deemed appropriate. 45 C.F.R. § 312(e)(2)(ii). In the Preamble, at 8,357, HHS explained that it dropped the proposed requirement for encryption, making it addressable instead, because the Department recognized the technological and financial "burdens" such a mandate might bring, and because it agreed that certain types of transmissions had a very low risk of interception. The decision also took into account the fact that as of February 2003 "there is not yet available a simple and interoperational solution to encrypting email communication with patients [or plan members]." The Preamble (id.) goes on to say that "covered entities are encouraged, however, to consider use of encryption technology for transmitting EPHI, particularly over the Internet." The HHS Interim Rule on

[12] *Id.* at 86.
[13] *Id.* at 86.
[14] *Id.* at 86.

TECHNICAL SAFEGUARDS

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304

	Security Standard	*Implementation Specifications*	*Explanation*
			Breach Notification for Unsecured Protected Health Information published at 74 Fed. Reg. 42,740 (August 24, 2009) highlights the current importance of encrypting EPHI. If implementing an encryption scheme for EPHI transmitted over a network is reasonable and appropriate, then the EPHI must be encrypted (e.g., public/private keys). Considerations regarding the reasonableness and appropriateness of encrypting EPHI include the following: • The recipient's ability to receive and decrypt an encrypted message; • The sensitivity of the transmitted information; • The potential impact of unauthorized EPHI disclosure; • The costs of implementing, managing, and operating the encryption system; and • The vulnerabilities of the network and overall environment.[15] If encryption of EPHI is feasible, then transmission of all data must be encrypted including, but not limited to, e-mail, web transmissions, and other data transmissions[16] (e.g., uploading, downloading, streaming, etc.).
		Encryption (Addressable) 45 C.F.R. § 312(e)(2)(ii)	Implement a mechanism to encrypt EPHI whenever deemed appropriate." In the Preamble, at 8,357, HHS explained that it dropped the proposed requirement for encryption, making it addressable instead, because the Department recognized the technological and financial "burdens" such a mandate might bring, and because it agreed that certain types of transmissions had a very low risk of interception. The decision also took into account the fact that "there is not yet available a simple and interoperational solution to encrypting email communication with patients [or plan members]." The Preamble (id.) goes on to say that "covered entities are encouraged, however, to consider use of encryption technology for transmitting EPHI, particularly over the Internet."

[15] *Id.* at 87-88.
[16] *Id.* at 88.

SECURITY INCIDENTS

Current Business Associate Contract Obligation	**HITECH Act Obligation (Sec. 13401(a) quoted to the right) – effective 2/17/2010**	“Section 164.308 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity.”	
	Security Standard	*Implementation Specifications*	*Explanation*
BA agrees to report to CE any **security incident** involving EPHI of which it becomes aware. 45 C.F.R. § 164.314(a)(2)(i)(C).	Security Incidents Procedure 45 C.F.R. § 164.308(a)(6) “Implement policies and procedures to address security incidents.” The Security Rule, 45 C.F.R. § 164.304, defines a “security incident” as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." According to the Preamble at 8,350, this also includes improper network activity and misuse of outside data. HHS expects Covered Entities to judge for themselves what is a security incident. According to the Preamble, at 8,350, “an entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.”	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.” The Security Rule does not require that CEs report such incidents to outside entities, but HHS notes that such reporting may be necessary "based on business and legal considerations." Id. In contrast, the Security Rule’s BA provision obligates the BA to report security incidents to the impacted CE.

SUB-BUSINESS ASSOCIATES

Current Contractual Obligation	**HITECH Act Obligation (Note: This obligation falls under Administrative Safeguards)**		
	Security Standard	*Implementation Specifications*	*Explanation*
BA will ensure that any agent, including a subcontractor, to whom it provides [EPHI] agrees to implement reasonable and appropriate safeguards to protect it. 45 C.F.R. § 164.314(2)(i)(B).	Business Associate Contracts 45 C.F.R. § 164.308(b)(1) A Covered Entity, in accordance with § 164.306, may only permit a Business Associate to create, receive, maintain, or transmit EPHI 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. The term “Business Associate” has the same meaning under the Security Rule as it has under the Privacy Rule. 45 C.F.R. § 160.103	Written Contract or Other Arrangements (Required) 45 C.F.R. § 164.308(b)(2)	Covered Entities must document the satisfactory assurances required by §164.308(b)(1) through a written contract or other arrangement (in the case of government entities) with the business associate that meets the applicable requirements of § 164.314(a), specifically (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 [the Security Rule]; (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.

POLICIES AND PROCEDURES

Current Business Associate Contract Obligation	**HITECH Act Obligation (Sec. 13401(a) quoted to the right) – effective 2/17/2010**	“Section 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity.”	
	Security Standard	*Implementation Specifications*	*Explanation*
None	Policies and procedures requirements 45 C.F.R. § 164.316(a)	No implementation specifications for this standard	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule, taking into account those factors specified in 45 C.F.R. § 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. An entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance the Security Rule. These documentation requirements obligate entities to locate and otherwise prepare documentation on currently undocumented procedures as well as others deemed necessary through the risk analysis and management processes. HHS advises in the Preamble, at 8,361, that the required “documentation must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations.”
	Documentation 45 C.F.R. § 164.316(b)(1) **“**Maintain the policies and procedures implemented to comply with the Security Rule in written (which may be electronic) form; and 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.”	Time limit (Required) 45 C.F.R. § 164.316(b)(1)(i)	“Retain the required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.”
		Availability (Required) 45 C.F.R. § 164.316(b)(1)(ii)	“Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.”
		Updates (Required) 45 C.F.R. § 164.316(b)(iii)	“Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI.”