**HITECH/HIPAA Business Associates**

**Gap Analysis Checklist Version 2.1**

**January 7, 2010**

The following checklist is intended for use in a gap analysis of Business Associate compliance under Subtitle D of the Health Information for Economic and Clinical Health (“HITECH”) Act, the HIPAA regulations it incorporates, and other directly applicable regulations and regulatory guidance.

Each row stands for a specific compliance requirement. Each requirement is identified by citation to the HITECH or HIPAA provision and its title, and includes a description of the requirement. The “Status/Comment” field for each requirement is to be filled in by the assessor with information about the entity’s status with respect to the requirement. A gray cell indicates that the requirement is a general one, which has compliance specifications in subsequent cells where status and comments should be indicated.

Information for gap analysis should be obtained by review of the entity’s written policies, procedures, guidelines, standards or other documentation applicable to each requirement. If documentation is not available, that should be noted, as lack of documentation may itself be a material gap. Physical security should be assessed by walk-through and observation of relevant facilities, and technical security by review of systems architectures, operating systems and applications. Key personnel should be interviewed to ensure accurate information about relevant documentation, practices, processes and systems, but personal knowledge about undocumented practices for compliance with material requirements should not be considered sufficient to meet such requirements. This checklist is not intended to be used to audit compliance with existing policies and procedures, but to support remediation and compliance.

THIS CHECKLIST IS NOT PROVIDED AS LEGAL ADVICE OR INTENDED FOR USE BY ANY SPECIFIC ENTITY, OPERATING ENVIRONMENT OR SYSTEMS ARCHITECTURE. IT IS INTENDED TO PROVIDE EDUCATIONAL SUPPORT AND GENERAL INFORMATION, AND IS PROVIDED “AS IS.”

For additional information please contact the author.

| **Citation** | **Title** | **Description** | **Status/Comments** |
| --- | --- | --- | --- |
| HITECH § 13401(a) | Application of Security Provisions and Penalties to Business Associates | “Sections 164.308, 164.310, 164.312, and 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.” |  |
| HIPAA 45 C.F.R. § 164.308 | Administrative Safeguards |  |  |
| HIPAA 45 C.F.R. § 164.308(a)(1) | Security Management Process | “Implement policies and procedures to prevent, detect, contain, and correct security violations.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(1)(ii)(A) | Risk Analysis (Required) | “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of 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 (Preamble, at 8,347), such as “losses caused by inappropriate uses and disclosures and the loss of data integrity that would occur absent the security measures.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(1)(ii)(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).” |  |
| HIPAA 45 C.F.R. § 164.308(a)(1)(ii)(C) | Sanction Policy (Required) | “Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.” 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. |  |
| HIPAA 45 C.F.R. § 164.308(a)(1)(ii)(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.” 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.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(2) | Assigned Security Responsibility (Required) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(3)(i) | Workforce Security |  |  |
| HIPAA 45 C.F.R. § 164.308(a)(3)(ii)(A) | Authorization and/or Supervision (Addressable) | “Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where EPHI might be accessed” |  |
| HIPAA 45 C.F.R. § 164.308(a)(3)(ii)(B) | Workforce Clearance Procedure (Addressable) | “Implement procedures to determine that the access of a workforce member to EPHI is appropriate.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(3)(ii)(C) | Termination Procedures (Addressable) | “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]”. |  |
| HIPAA 45 C.F.R. § 164.308(a)(4)(i) | Information Access Management | “Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of [the Privacy Rule].” |  |
| HIPAA 45 C.F.R. § 164.308(a)(4)(ii)(B) | Access Authorization (Addressable) | Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(4)(ii)(C) | Access Establishment and Modification (Addressable) | “Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(5)(i) | Security Awareness and Training | “Implement a security awareness and training program for all members of its workforce (including management).” |  |
| HIPAA 45 C.F.R. § 164.308(a)(5)(i) | Security Reminders (Addressable) | Provide periodic security updates to the workforce. |  |
| HIPAA 45 C.F.R. § 164.308(a)(5)(ii)(A) | Protection from Malicious Software (Addressable) | “Implement procedures for guarding against, detecting, and reporting malicious software.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(5)(ii)(B) | Log-in Monitoring (Addressable) | “Implement procedures for monitoring log- in attempts and reporting discrepancies.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(5)(ii)(C) | Password Management (Addressable)  | “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. |  |
| HIPAA 45 C.F.R. § 164.308(a)(6)(i) | Security Incident Procedures | “Implement policies and procedures to address security incidents”[[1]](#footnote-1) |  |
| HIPAA 45 C.F.R. § 164.308(a)(6)(ii)(A) | 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” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(i) | 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 EPHI.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(ii)(A) | Data Backup Plan (Required) | “Establish and implement procedures to create and maintain retrievable exact copies of EPHI” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(ii)(B) | Disaster Recovery Plan (Required) | “Establish (and implement as needed) procedures to restore any loss of data.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(ii)(C) | Emergency Mode Operation Plan (Required) | “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.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(ii)(D) | Testing and Revision Procedure (Addressable) | “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.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(7)(ii)(E) | Applications and Data Criticality Analysis (Addressable) | “Assess the relative criticality of specific applications and data in support of other contingency plan components.” |  |
| HIPAA 45 C.F.R. § 164.308(a)(8) | Evaluation | “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.” |  |
| HIPAA 45 C.F.R. § 164.308(b)(1) | Business Associate Contracts[[2]](#footnote-2) | “A covered entity, in accordance with [45 C.F.R. § 164.306], may 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 [45 C.F.R. § 164.314(a) that the business associate will appropriately safeguard the information” |  |
| HIPAA 45 C.F.R. § 164.310 | Physical Safeguards |  |  |
| HIPAA 45 C.F.R. § 164.310(a)(1) | 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.” |  |
| HIPAA 45 C.F.R. § 164.310(a)(2)(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.” |  |
| HIPAA 45 C.F.R. § 164.310(a)(2)(ii) | Facility Security Plan (Addressable) | “Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.” |  |
| HIPAA 45 C.F.R. § 164.310(a)(2)(iii) | Access Control & Validation Procedure (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.” |  |
| HIPAA 45 C.F.R. § 164.310(a)(2)(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).” |  |
| HIPAA 45 C.F.R. § 164.310(b) | Workstation Use (Required) | “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.” |  |
| HIPAA 45 C.F.R. § 164.310(c) | Workstation Security (Required) | “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. |  |
| HIPAA 45 C.F.R. § 164.310(d)(1) | Device and Media Controls | “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.” |  |
| HIPAA 45 C.F.R. § 164.310(d)(2)(i) | Disposal (Required) | “Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.” |  |
| HIPAA 45 C.F.R. § 164.310(d)(2)(ii) | Media Re-use (Required) | “Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.” |  |
| HIPAA 45 C.F.R. § 164.310(d)(2)(iii) | Accountability (Addressable) | “Maintain a record of the movements of hardware and electronic media and any person responsible therefore.” |  |
| HIPAA 45 C.F.R. § 164.310(d)(2)(iv) | Data Backup and Storage (Addressable) | “Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.” |  |
| HIPAA 45 C.F.R. § 312 | Technical Safeguards |  |  |
| HIPAA 45 C.F.R. § 312(a)(1) | Access Control | “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 [45 C.F.R.] § 164.308(a)(4).” |  |
| HIPAA 45 C.F.R. § 312(a)(2)(i) | Unique User Identification (Required) | “Assign a unique name and/or number for identifying and tracking user identity.” |  |
| HIPAA 45 C.F.R. § 312(a)(2)(ii) | Emergency Access Procedure (Required) | “Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.”[[3]](#footnote-3) |  |
| HIPAA 45 C.F.R. § 312(a)(2)(iii) | Automatic Logoff (Addressable) | “Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.” |  |
| HIPAA 45 C.F.R. § 312(a)(2)(iv) | Encryption and Decryption (Addressable) | “Implement a mechanism to encrypt and decrypt EPHI.”[[4]](#footnote-4) |  |
| HIPAA 45 C.F.R. § 312(b) | Audit Controls (Required) | “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.” |  |
| HIPAA 45 C.F.R. § 312(c)(1) | Integrity | “Implement policies and procedures to protect EPHI from improper alteration or destruction.” |  |
| HIPAA 45 C.F.R. § 312(c)(2) | Mechanism to Authenticate Electronic PHI (Addressable) | “Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. |  |
| HIPAA 45 C.F.R. § 312(d) | Person or Entity Authentication (Required) | “Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.” |  |
| HIPAA 45 C.F.R. § 312(e)(1) | Transmission Security | “Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.” |  |
| HIPAA 45 C.F.R. § 312(e)(2)(i) | Integrity Controls (Addressable) |  “Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.” |  |
| HIPAA 45 C.F.R. § 312(e)(2)(ii) | Encryption (Addressable) | “Implement a mechanism to encrypt EPHI whenever deemed appropriate.”[[5]](#footnote-5) |  |
| HIPAA 45 C.F.R. § 164.316 | Policies and Procedures and Documentation Requirements |  |  |
| HIPAA 45 C.F.R. § 164.316(a) | Policies and Procedures | “Implement reasonable and appropriate policies and procedures to comply with the . . . the requirements of [the HIPAA security regulations] |  |
| HIPAA 45 C.F.R. § 164.316(b)(1)(i) |  | “Maintain the policies and procedures implemented to comply with [the HIPAA security regulations] in written (which may be electronic) form” |  |
| HIPAA 45 C.F.R. § 164.316(b)(1)(ii) |  | “”If an action, activity, or assessment is required by [the HIPAA security regulations] to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment”[[6]](#footnote-6) |  |
| HIPAA 45 C.F.R. § 164.316(b)(2)(i) | Time Limit (Required) | Required documentation to be retained at least six years “from the date of its creation or the date when it was last in effect, whichever is later” |  |
| HIPAA 45 C.F.R. § 164.316(b)(2)(ii) | Availability (Required) | “Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains” |  |
| HIPAA 45 C.F.R. § 164.316(b)(2)(ii) | Updated (Required) | “Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the [ePHI]” |  |
| HITECH § 13401(a) | Application of Security Provisions and Penalties to Business Associates | “The additional requirements of this title [HITECH] that relate to security and that are made applicable with respect to covered entities . . . shall be incorporated into the business associate agreement between the business associate and the covered entity.” |  |
| HITECH § 13402(b) | Notification in the Case of Breach / Business Associates | “A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.”[[7]](#footnote-7) |  |
| 45 C.F.R. Parts 160 and 164 | Breach Notification for Unsecured Protected Health Information; Interim Final Rule |  |  |
| 45 C.F.R § 164.402 | Definitions | Breach does not include “use or disclosure of [PHI] that does not include the code identifiers listed at [45 C.F.R.] §164.514(e)(2)”[[8]](#footnote-8) |  |
| 45 C.F.R § 164.402 | Definitions | Breach does not include “use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under [the HIPAA privacy regulations]” |  |
| 45 C.F.R § 164.402 | Definitions | “Unsecured [PHI] means [PHI] that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under [HITECH § 13402(h)(2)]” |  |
| 45 C.F.R § 164.410 | Notification by a business associate. | “A business associate discovery of a breach of unsecured protected health information, notify the covered entity of such breach.”“A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).” |  |
| HITECH § 13402(h) Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals  | NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices. | Encryption standards for ePHI at rest[[9]](#footnote-9) |  |
| HITECH § 13402(h) Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals  | NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800– 77, Guide to IPsec VPNs; or 800–113, Guide to SSL VPNs | Encryption standards for ePHI in transmission[[10]](#footnote-10) |  |
| HITECH § 13402(h) Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals | NIST Special Publication 800–88, Guidelines for Media Sanitization | “Electronic media have been cleared, purged, or destroyed” prior to disposal so that ePHI is not recoverable”[[11]](#footnote-11) |  |
| HITECH § 13402(h) Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals | Paper, other non-electronic media sanitization | “Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction” |  |
| HITECH § 13404(a) | Application of Privacy Provisions and Penalties to Business Associates of Covered Entities | “In the case of a business associate of a covered entity that obtains or creates [PHI] pursuant to a written contract . . . described in [45 C.F.R. §] 164.502(e)(2) . . . the business associate may use and disclose such [PHI] only if such use or disclosure, respectively, is in compliance with each applicable requirement of [45 C.F.R. §] 164.504(e)” |  |
| HIPAA 45 C.F.R. § 164.504(e)(1) | Business Associate Contracts | “The contract . . . between the covered entity and the business associate . . . must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.” |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(i) | Business Associate Contracts | Business Associate Contract must “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,” but may “permit the business associate to use and disclose [PHI] for the proper management and administration of the business associate” and to “provide data aggregation services relating to the health care operations of the covered entity.” |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(A) | Business Associate Contracts | Business Associate may not “use or further disclose the information other than as permitted or required by the contract or as required by law” |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(B) | Business Associate Contracts | Business Associate must “use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract”[[12]](#footnote-12) |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(C) | Business Associate Contracts | Business Associate must “report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware”[[13]](#footnote-13) |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(D) | Business Associate Contracts | Business Associate must “ensure that any agents, including a subcontractor, to whom it provides [PHI] 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”[[14]](#footnote-14) |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(E) | Business Associate Contracts | Business Associate must make PHI available for access and copying by individual data subjects, subject to health care provider’s denial of access due to potential danger to “life or physical safety” |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(F) | Business Associate Contracts | Business Associate must make PHI available for amendment by individual data subjects, and incorporate amendments accepted by Covered Entity |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(G) | Business Associate Contracts | Business Associate must make accounting of disclosures available to individual data subjects, for all disclosure other than for treatment, payment or health care operations, and for other limited purposes not including research |  |
| HIPAA 45 C.F.R. §164.504(e)(2)(ii)(H) | Business Associate Contracts | Business Associate must make its own internal books and records available for regulatory audit of Covered Entity compliance[[15]](#footnote-15) |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(ii)(I) | Business Associate Contracts | Business Associate must, “at termination of the contract, if feasible, return or destroy all [PHI] 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”[[16]](#footnote-16) |  |
| HIPAA 45 C.F.R. § 164.504(e)(2)(iii) | Business Associate Contracts | Business Associate Contract must “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”[[17]](#footnote-17)20 |  |
| HITECH § 13404(a) | Application of Privacy Provisions and Penalties to Business Associates of Covered Entities | “The additional requirements of [Subtitle D] that relate to privacy and that are made applicable with respect to covered entities . . . shall be incorporated into the business associate agreement between the business associate and the covered entity |  |
| HITECH § 13404(b) | Application of Knowledge Elements Associated with Contracts | Business Associate Contracts must have provision reciprocal to Covered Entity termination provision of 45 C.F.R. F §§ 164.314((2)(i)(D), .504(e)(2)(iii), so that Business Associate may terminate contract for uncured Covered Entity breach, or notify regulatory agency if termination not feasible |  |
| HITECH § 13405(b) | Disclosures Required to be Limited to the Limited Data Set or the Minimum Necessary | Covered Entities and Business Associates must limit PHI used, disclosed or requested to either (1) a limited data set as defined at HIPAA 45 C.F.R. 164.514(e)(2), or (2) the “minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively” |  |
| HIPAA 45 C.F.R. § 164.502(b) | Minimum Necessary | “When using or disclosing [PHI] or when requesting [PHI] from another covered entity, a covered entity must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure or request” Minimum necessary does not apply (1) to disclosures or requests by health care provider for treatment, (2) to disclosures to the data subject, (3) pursuant to an authorization by the individual, (4) for compliance purposes and (5) if required by law. |  |
| HIPAA 45 C.F.R. § 164.514(d)(2) | Minimum Necessary Requirements | Minimum necessary compliance requires (1) identification of persons or classes of persons who need access to PHI to carry out their duties; (2) specification for each of the category or categories of PHI to which access is needed and any conditions appropriate to such access; (3) policies and procedures to limit access according to such categories for routine transactions; and (4) criteria for determining minimum necessary for non-routine transactions. |  |
| HIPAA 45 C.F.R. § 164.514(d)(3) | Minimum Necessary Requirements | For research purposes, a Covered Entity may rely on “documentation or representations that comply with the applicable requirements of [45 CFR] § 164.512(i)” to establish the minimum necessary PHI |
| HIPAA 45 C.F.R. § 164.514(e)(1) | Limited Data Sets | “A covered entity may use or disclose a limited data set . . . if the covered entity enters into a data use agreement with the limited data set recipient” |  |
| HIPAA 45 C.F.R. § 164.514(e)(2) | Limited Data Sets | Limited data set excludes most identifiers, does allow dates, identification codes |  |
| HIPAA 45 C.F.R. § 164.514(e)(3) | Permitted Uses and Disclosures of Limited Data Sets | Includes research |  |
| HIPAA 45 C.F.R. § 164.514(e)(4) | Limited Data Set Agreements | Use or disclosure of limited data sets requires limited data set with mandatory provisions |  |
| HITECH § 13405(d)(1) | Prohibition on Sale of Electronic Health Records or Protected Health Information | “A covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual . . . a valid authorization that includes . . . a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that individual” |  |
| HITECH § 13405(d)(2)(B) | Exception for Research | Not applicable if “the purpose of the exchange is for research [as defined under HIPAA] and the price charged reflects the costs of preparation and transmittal of the data for such purpose” |  |
| HITECH § 13405(d)(2)(C) | Exception for Treatment | Not applicable if “the purpose of the exchange is for the treatment of the individual, subject to any regulation that [OCR] may promulgate to prevent protected health information from inappropriate access, use, or disclosure” |  |
| HITECH § 13405(d)(2)(E) | Exception for Business Associate Services | Not applicable if “the purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement” |  |

1. Cross-reference to HITECH § 13402, re notification of security breaches [↑](#footnote-ref-1)
2. It is not clear how this requirement should be treated since HITECH § 13401(a) did not refer to 45 C.F.R. §§ 164.306 and 314. If this requirement is applicable to Business Associates, it appears to mean that the Business Associate Contracts required by 45 C.F.R. § 164.314(a)(2), including provisions for Business Associate safeguards, implementation of safeguards by Business Associates subcontractors obtaining PHI, security incident reporting and termination for Business Associate breach of the Business Associate Contract, would be applied to subcontractors as if they were Business Associates within the meaning of the regulation [↑](#footnote-ref-2)
3. Cross-reference to contingency planning requirements at 45 C.F.R. § 164.308(a)(7)(i). [↑](#footnote-ref-3)
4. Cross-reference to HITECH Security Breach Guidance encryption standards. [↑](#footnote-ref-4)
5. Note need for careful cross-references of documentation requirements, e.g. of user access authorization per HIPAA 45 C.F.R. § 164.308(a)(4)(ii)(C), security incident response per HIPAA 45 C.F.R. § 164.308(a(6)(ii), maintenance records per HIPAA 45 C.F.R. § 164.310((a)(2(iv), etc. Note also that Covered Entity HIPAA security safeguards determinations may include documented determinations to implement alternative safeguards for “addressable” specifications under HIPAA 45 C.F.R. § 164.306(d)(ii)(3), which HITECH § 13401(a) did not reference. It is not clear whether this means Business Associates cannot implement alternative safeguards for addressable specifications, but in any case where that approach is contemplated appropriate documentation would be prudent. [↑](#footnote-ref-5)
6. Cross-reference to safeguards evaluation requirement of HIPAA 45 C.F.R. § 164.308(a)(8). [↑](#footnote-ref-6)
7. Cross-reference HIPAA Business Associate security incident reporting, 45 C.F.R § 164.308(a)(6)(ii)(A). [↑](#footnote-ref-7)
8. Reference is to HIPAA privacy regulation defining acceptable de-identification of PHI. [↑](#footnote-ref-8)
9. Cross-reference to HIPAA encryption requirement, 45 C.F.R. § 164.312(a)(2)(iv). [↑](#footnote-ref-9)
10. Cross-reference to HIPAA encryption requirement, 45 C.F.R. § 164.312(e)(2)(ii). [↑](#footnote-ref-10)
11. Cross-reference to HIPAA disposal requirement, 45 C.F.R. § 164.310(d)(2)(ii). [↑](#footnote-ref-11)
12. Cross-reference to HITECH § 13401(a) requirement for HIPAA security regulation compliance; note that this provision also applies to non-electronic PHI (paper, film, oral, etc.). [↑](#footnote-ref-12)
13. Cross-reference to HITECH § 13402 requirement for security breach notification and HIPAA security rule requirement for business associate security incident reporting at 45 C.F.R. § 164.314(a)(2)(i)(C). [↑](#footnote-ref-13)
14. Cross-reference to comparable HIPAA security rule requirement at 45 C.F.R. § 154.314(a)(2)(i)(B). [↑](#footnote-ref-14)
15. Cross-reference HITECH § 13411, providing for audits of both Covered Entities and Business Associates. [↑](#footnote-ref-15)
16. Cross-reference media sanitization guidance for HITECH § 13402 and media disposal requirements of HIPAA security rule, 45 C.F.R. § 164.310(d). [↑](#footnote-ref-16)
17. Cross-reference reciprocal requirement of Business Associate termination in HITECH § 13404(b) and comparable HIPAA security rule requirement at 45

C.F.R. § 164.314(a)(2)(i)(D). [↑](#footnote-ref-17)