Structuring Business Associate Agreements for Covered Entities and Business Associates
Navigating Regulatory Compliance and Negotiating Key Provisions

MONDAY, DECEMBER 21, 2015

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:

Gerry Hinkley, Partner, Pillsbury Winthrop Shaw Pittman, Los Angeles

Kim C. Stanger, Partner, Holland & Hart, Boise, Idaho

Allen Briskin, Senior Counsel, Pillsbury Winthrop Shaw Pittman, Los Angeles

Rick L. Hindmand, Member, McDonald Hopkins, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Avoiding Business Associate Agreements

11/26/2013
by Kim Stanger

The HIPAA privacy rules now apply to both covered entities (e.g., healthcare providers and health plans) and their business associates. A "business associate" is generally a person or entity who "creates, receives, maintains or transmits" protected health information ("PHI") in the course of performing services on behalf of the covered entity (e.g., consultants; management, billing, coding, transcription or marketing companies; information technology contractors; data storage or document destruction companies; data transmission companies or vendors who routinely access PHI; third party administrators; personal health record vendors; lawyers; accountants; malpractice insurers; etc.) (See 45 CFR 160.103). "A covered entity may be a business associate of another covered entity." (Id.). Also, with very limited exceptions, a subcontractor or other entity that creates, receives, maintains or transmits PHI on behalf of a business associate is also a business associate. (Id.; 78 FR 5572). To determine if an entity is a business associate, see the attached Business Associate Decision Tree.

Business Associate Requirements. In general, an entity that is a "business associate" under HIPAA must do the following:


2. Implement specified administrative, technical and physical safeguards to protect the integrity, confidentiality, and availability of electronic PHI (e.g., establish access controls; use firewalls, virus protections, and encryption; backup data; implement appropriate security policies and procedures; etc.). (45 CFR 164.300 et seq.).

3. Execute and perform according to written business associate agreements with covered entities that essentially require the business associate to maintain the privacy of PHI; limit the business associate's use or disclosure of PHI to those purposes authorized by the covered entity; and assist covered entities in responding to patient requests concerning their PHI. (45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e)). For more information about business associate agreements, see the attached Checklist for HIPAA Business Associate
**Agreements.** If the covered entity discloses only a "limited data set" to
the business associate, the parties may execute a data use agreement
instead of a full business associate agreement. (45 CFR 164.514(e)).

4. Report security incidents and privacy breaches to the covered
entity. (45 CFR 164.314(a), 164.410, and 164.502(e)).

5. If the business associate uses subcontractors or other entities to
provide any services for the covered entity involving PHI, execute
business associate agreements with the subcontractors. (45 CFR
164.314(a) and 164.504(e)).

Business associates who violate HIPAA may be subject to penalties of
$100 to over $50,000 per violation. (45 CFR 160.404). If the violation
resulted from willful neglect, the Office of Civil Rights ("OCR") must
impose a penalty of at least $10,000 per violation. (Id.). If the business
associate acted with willful neglect and fails to correct the violation
within thirty (30) days, the OCR must impose a penalty of at least
$50,000 per violation. (Id.). A single breach may result in numerous
violations. For example, the loss of a laptop containing hundreds of
patients' PHI may constitute hundreds of violations. Similarly, each day
that a covered entity or business associate fails to implement a
required policy constitutes a separate violation. (45 CFR 160.406). In
addition to regulatory penalties, business associates who fail to
comply with business associate agreements may also be liable for
contract damages and/or indemnification requirements set forth in
the business associate agreement.

**Avoiding Business Associate Requirements.** Given the cost of
compliance and penalties for noncompliance, entities may want to
avoid becoming a "business associate" or executing business associate
agreements if possible. The following are not business associates and
may properly decline to execute a business associate agreement:

1. **Entities that do not create, receive, maintain, or transmit PHI.** If
you want to avoid business associate obligations, the safest course is
to ensure that you do not handle PHI on behalf of either a covered
entity or a business associate of a covered entity. Accidental receipt of
or incidental access to PHI outside your contracted job duties does not
trigger business associate obligations. The OCR has stated:

A business associate contract is not required with persons or
organizations whose functions, activities, or services do not
involve the use or disclosure of [PHI], and where any access to
[PHI] by such persons would be incidental, if at all. [For example],
janitorial services that clean the offices or facilities of a covered
entity are not business associates because the work they perform
for covered entities does not involve the use or disclosure of
[PHI], and any disclosure of [PHI] to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented.

(OCR Frequently Asked Questions ("FAQ"), available at http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html). Similarly, "[t]he mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the [PHI] of the covered entity." (Id.). Entities seeking to avoid business associate obligations may want to include a provision in their service contracts confirming that they do not require PHI to perform their functions, and that its clients who are covered entities or business associates will not provide PHI (or, as discussed below, unencrypted PHI) to the entity without the entity's prior agreement.

2. Members of an entity's own workforce. Members of an entity's own workforce are not business associates of the entity, including "employees, volunteers, trainees, and other persons whose conduct, in performance of work for a covered entity or business associate, is under the direct control of such entity or business associate, whether or not they are paid by the covered entity or business associate." (45 CFR 160.103). To avoid business associate obligations, contractors may seek to be classified as members of the covered entity's workforce. The OCR has stated:

If a service is hired to do work for a covered entity where disclosure of [PHI] is not limited in nature (such as routine handling of records or shredding of documents containing [PHI]), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.

(OCR FAQ; see also 78 FR 5574). Similarly,

A software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to [PHI]. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at
a covered entity, the covered entity may choose to treat the
employee of the vendor as a member of the covered entity's
workforce, rather than as a business associate.

(OCR FAQ). Although characterization as a workforce member would help contractors avoid business associate obligations, covered entities may resist classifying contractors as members of their workforce because doing so may indicate that the contractor is acting as the agent of the covered entity, thereby exposing the covered entity to vicarious liability for the contractor's actions. (See 45 CFR 160.402(c); 78 FR 5581).

3. Members of an organized health care arrangement. Covered entities that participate in an organized health care arrangement ("OHCA") are not business associates of each other while performing functions on behalf of the OHCA; "thus, they may use and disclose [PHI] for the joint health care activities of the OHCA without entering into a business associate agreement." (OCR FAQ; see 45 CFR 160.103). An OHCA is (1) "A clinically integrated care setting in which individuals typically receive health care from more than one health care provider" (e.g., a hospital and its medical staff); (2) an organized system of health care in which more than one covered entity participates and in which the participating covered entities engage in joint utilization review, quality improvement, or payment activities (e.g., provider networks); or (3) certain arrangements between group health plans and other insurers. (45 CFR 160.103). The OHCA exception only applies to covered entities (e.g., healthcare providers and health plans) that perform functions for the OHCA; it does not apply to other entities that require PHI to perform functions on behalf of the OHCA.

4. Healthcare providers who receive PHI to treat patients. A healthcare provider is not a business associate of other covered entities while rendering treatment to patients. (See 45 CFR 160.103; see also 65 FR 82476 and 82504). As explained by the OCR:

The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share [PHI] with a health care provider for treatment purposes without a business associate contract.

(OCR FAQ). For example,

- A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
• A physician is not required to have a business associate contract with a laboratory as a condition of disclosing [PHI] for the treatment of an individual.

• A hospital laboratory is not required to have a business associate contract to disclose [PHI] to a reference laboratory for treatment of the individual.

(OCR Business Associate Guidance, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html). This exception only applies to the extent that the healthcare provider is using the PHI for treatment purposes; it would not apply if the healthcare provider is using the information to perform other functions on behalf of the covered entity. "For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to [PHI]." (OCR FAQ). Even in that example, however, the hospital and physician would not need a business associate agreement if they were members of an OHCA.

5. Entities acting on their own behalf or on behalf of the patient. The business associate requirements only apply to entities who are performing a function involving PHI on behalf of a covered entity or its business associate. Entities that handle PHI for their own purposes are not business associates. For example, "[a] provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the 'business associate' of the other." (OCR Business Associate Guidance). Similarly, a bank or financial institution is not a business associate of a covered entity when it "processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums"; in such cases, "the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity" and is not a business associate. (Id.; 78 FR 5575; 65 FR 82476). Researchers are not business associates of covered entities even if the researcher is hired by the covered entity to conduct research. (78 FR 5575). "Where a physician or other provider has staff privileges at an institution, neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other." (65 FR 82476). Covered entities that simply provide PHI for another covered entity’s healthcare operations are not business associates of the other entity. (65 FR 82476). Finally, an entity performing services on behalf of the patient, not on behalf of
the healthcare provider, is not a business associate (e.g., an attorney who requests health information to represent the patient, or a company that collects and interprets data on behalf of a patient).

6. Entities performing management or administrative functions for business associates. Covered entities may allow business associates to use PHI for the business associate's own management and administration or legal responsibilities. (45 CFR 164.504(e)(4)). If so, disclosures by a business associate ... for its own management and administration or legal responsibilities do not create a business associate relationship with the recipient of the [PHI] because such disclosures are made outside of the entity's role as a business associate.... In contrast, disclosures of [PHI] by the business associate to a person who will assist the business associate in performing a function, activity, or service for a covered entity or another business associate may create a business associate relationship depending on the circumstances. (78 FR 5574). However, even if no business associate agreement is required because an entity is assisting the business associate in its own management or administration functions, HIPAA still restricts the use or disclosure of PHI by the entity:

for [any] such disclosures that are not required by law, [HIPAA] requires that the business associate obtain reasonable assurances from the person to whom the [PHI] is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person notifies the business associate of any instances of which it is aware that the confidentiality of the information has been breached. See § 164.504(e)(4)(ii)(B).

(78 FR 5574). Such "reasonable assurances" may be obtained through a limited confidentiality agreement; a full-blown business associate agreement is not required.

7. Entities who are mere "conduits" for PHI. Entities that transmit PHI for a covered entity are not business associates if they are not required to access the PHI on a routine basis, i.e., they are merely "conduits" of the PHI (e.g., internet service providers, phone companies, etc.). (45 CFR 160.103; 78 FR 5571; 65 FR 82476).

Regarding what it means to have "access on a routine basis" to [PHI] with respect to determining which types of data transmission services are business associates versus mere conduits, such a determination will be fact specific based on the
nature of the services provided and the extent to which the entity needs access to [PHI] to perform the service for the covered entity. The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to [PHI] when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to [PHI] would not qualify the company as a business associate. In contrast, an entity that requires access to [PHI] in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of [PHI] through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate.

(78 FR 5571-72).

8. **Maybe entities who maintain encrypted PHI.** In contrast to entities that transmit PHI, entities that maintain PHI (e.g., data storage companies) are generally considered business associates. (45 CFR 160.103; 78 FR 5572). As HHS explained:

an entity that maintains [PHI] on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the [PHI]. We recognize that in both situations, the entity providing the service to the covered entity has the opportunity to access the [PHI]. However, the difference between the two situations is the transient versus persistent nature of that opportunity. For example, a data storage company that has access to [PHI] (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining [PHI] on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold.

(78 FR 5572, emphasis added). Note that the foregoing analysis applies to data storage companies that "have access to" the PHI. Unless and until we receive contrary guidance from HHS, there is a fairly strong argument that business associate requirements do not and should not apply to entities that maintain encrypted PHI if the entity does not
have the encryption key. HHS's breach notification rule assumes that encrypted data is secure. (See OCR Guidance at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/bguidance.html). Accordingly, it would be consistent to assume that maintenance of encrypted data without the key should not trigger business associate obligations.

Avoiding Unnecessary Business Associate Agreements. Unfortunately, out of ignorance or an abundance of caution, many covered entities or business associates are requesting business associate agreements even when such agreements are not technically required. Entities should avoid executing unnecessary business associate agreements; doing so may subject them to contractual liabilities they would not have but for the agreement, including the costs of complying with regulations that do not otherwise apply; limits on the use of disclosure of information; and damages for failure to comply. In addition, by executing unnecessary business associate agreements, the entity may be inappropriately admitting that it is a business associate, thereby exposing itself to HIPAA penalties for noncompliance. To avoid such situations, entities who are asked to execute unnecessary business associate agreements might consider responding as follows:

1. Explain the limits on business associate obligations discussed above. Hopefully, the covered entity will recognize that a business associate agreement is not required, and will be willing to forego the agreement.

2. Explain the limits on the covered entity's liability. Some covered entities or business associates insist on business associate agreements because they mistakenly assume that they are vicariously liable for the contractor's HIPAA violations. HIPAA clearly states that covered entities or business associates are only liable for their business associates' or subcontractors' actions if the business associate or subcontractor is acting as an agent of the covered entity, i.e., that the covered entity had the right to control the business associate's or subcontractor's actions. (45 CFR 160.402(c); 78 FR 5581). The parties may avoid vicarious liability by ensuring that any contract between them clearly identifies the business associate or subcontractor as an independent contractor, not an agent, and that the covered entity does not control the actions or operations of the business associate or contractor. (78 FR 5581). To that end, an overly restrictive business associate agreement may actually work against the covered entity because it may suggest an agency relationship or give the covered entity greater control over the actions of the contractor.

3. Offer to execute an appropriate confidentiality agreement. In lieu of a business associate agreement, the business associate or
subcontractor might offer to enter an appropriate confidentiality agreement that protects the covered entity while avoiding the full responsibilities or regulatory liabilities of a business associate agreement.

4. Condition the business associate agreement. Finally, if the covered entity still insists on a business associate agreement, the business associate or subcontractor might minimize its exposure by conditioning a business associate agreement on the entity's status as a business associate, i.e., the entity undertakes the responsibilities if and to the extent that it is a business associate as defined by HIPAA. Although an imperfect solution, it might at least allow the entity to avoid regulatory penalties if it truly is not a business associate.

Conclusion and Caution. Hopefully, the foregoing will allow entities which truly are not "business associates" under HIPAA to avoid business associate status and associated liabilities. On the other hand, if an entity is truly a "business associate" under the regulations, it cannot escape regulatory liability by avoiding a business associate agreement. "[A] person or an entity is a business associate if the person or entity meets the definition of "business associate," even if a covered entity, or business associate with respect to a subcontractor, fails to enter into the required business associate contract with the person or entity." (78 FR 5574).

For questions regarding this update, please contact
Kim C. Stanger
Holland & Hart, U.S. Bank Plaza, 101 S. Capitol Boulevard, Suite 1400, Boise, ID 83702-7714
e-mail: kcstanger@hollandhart.com, phone: 208-383-3913
Business Associate Decision Tree

This decision tree will help you determine if an entity is a “business associate” under HIPAA, as defined in 45 CFR § 160.103

Will an entity (“Entity”) provide services to or on behalf of a Covered Entity? A “Covered Entity” is a healthcare provider or health plan, including most employee benefit plans.

[Note: This does not apply to (1) an employee, volunteer, trainee, or other person whose conduct is under the direct control of a Covered Entity (i.e., “workforce members”), (2) an Entity who is performing functions as part of a Covered Entity’s organized health care arrangement,1 or (3) Entities who receive info for their own purposes, and not to provide services to or on behalf of a Covered Entity (e.g., payors, government agencies, independent researchers, etc.).]

The Entity is not a business associate

Will the Entity create, receive, maintain or transmit protected health info (“PHI”) in the course of providing services to or on behalf of a Covered Entity?

[Note: This does not apply to Entities who may periodically see or hear PHI, but whose job duties for a Covered Entity do not involve the creation, receipt, maintenance, or transmission of PHI (e.g., a janitor, delivery person, or electrician who happens to be providing services in the building)].

The Entity is not a business associate

Is the Entity a healthcare provider who is receiving the PHI for purposes of treating the individual?

Yes

The Entity is not a business associate

No

Does the Entity perform a function or activity for the Covered Entity involving PHI that is regulated by HIPAA (e.g., healthcare operations or payment functions), including claims processing or administration; data analysis, processing or administration; or utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing services?

OR

Does the Entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a Covered Entity?

OR

Is the Entity a health information organization, e-prescribing gateway, or other Entity that provides data transmission services with respect to PHI and the Entity requires access to the PHI on a routine basis (i.e., the Entity is not merely the conduit for the PHI)?

OR

Does the outside entity person offer a personal health record to one or more individuals on behalf of a Covered Entity?

The Entity is a business associate. You must execute a valid business associate agreement with the Entity before disclosing PHI to the Entity. The business associate agreement must contain the elements in 45 CFR §§ 164.314(a) and 164.504(e)

The Entity is not a business associate
Organized health care arrangement means:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
2. An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
   (i) Hold themselves out to the public as participating in a joint arrangement; and
   (ii) Participate in joint activities that include at least one of the following:
       (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
       (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
       (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Checklist for HIPAA Business Associate Agreements

7/1/2013
by Kim Stanger

In the wake of the HITECH Act and recent Omnibus Rule changes, business associates of covered entities must comply with most of the HIPAA Privacy and Security Rules applicable to covered entities or face penalties of $100 to $50,000 per violation. Among other things, covered entities and business associates must execute agreements whereby the business associate agrees to comply with certain Privacy and Security Rule provisions affecting protected health information ("PHI"). The Omnibus Rules will require most covered entities and business associates to review and update their business associate agreements ("BAAs") by September 23, 2013. The Omnibus Rules will also require covered entities to execute BAAs with certain entities that were not considered business associates in the past, including data storage companies and entities that provide data transmission services and require access to the data on a routine basis. To see a decision tree for determining business associate status, click here.

Checklist for BAA Compliance. Under the HIPAA Privacy and Security Rules, BAAs generally must contain the following terms. To the extent the business associate enters a BAA with its subcontractors, those subcontract BAAAs should also contain equivalent terms.

1. Establish the permitted and required uses and disclosures of PHI by the business associate. The BAA may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the covered entity, except that the BAA may but is not required to:
   a. Permit the business associate to use and disclose PHI for the proper management and administration of the business associate.
   b. Permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
   c. Permit the business associate to disclose PHI for the foregoing purposes if (1) the disclosure is required by law, or (2)(i) the business associate obtains reasonable
assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and (ii) the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

2. Provide that the business associate will:\(^9\)
   a. Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law.
   b. Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.
   c. Where applicable, comply with Security Rules with respect to electronic PHI.
   d. Report to the covered entity any security incidents or use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured PHI as required by § 164.410.
   e. Ensure that any subcontractors that receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. Business associates may do so by requiring the subcontractors to execute a BAA with the business associate.
   f. Make available PHI consistent with the patient’s right to access PHI as set forth in § 164.524.
   g. Make available PHI for amendment and incorporate any amendments to PHI in accordance with § 164.526.
   h. Make available the information required to provide an accounting of disclosures in accordance with § 164.528, including certain information concerning disclosures of PHI in violation of the Privacy Rule.
   i. To the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation. [Note: this is a new requirement under the Omnibus Rule].
   j. Make its internal practices, books and records relating
to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of HHS for purposes of determining the covered entity's compliance with the Privacy Rule.

3. Include appropriate termination provisions\textsuperscript{10}, i.e.:

a. At termination of the contract, if feasible, the business associate must 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 PHI.

b. If such return or destruction of PHI is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

c. Authorize termination of the BAA by the covered entity if the covered entity determines that the business associate has violated a material term of the BAA.

Additional Terms. The OCR has published sample BAA language at its website, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. However, the OCR's sample language may not include additional terms that covered entities and business associates may want to include in their agreements. For example, while not required by HIPAA, covered entities may want to:

a. Confirm that the business associate is acting as an independent contractor and not as the agent of the covered entity.

b. Require business associates and subcontractors to carry appropriate insurance to cover HIPAA violations.

c. Require business associates and subcontractors to defend and indemnify the covered entity for violations of HIPAA or the BAA.

d. Require business associates, at their own cost, to respond to any potential HIPAA violation and provide any notice of privacy breaches or security incidents as mandated by the Privacy, Security or Breach Notification Rules.

e. Impose time limits or other conditions on the business associate's performance so long as such conditions do not
establish an agency relationship as discussed below.

f. Coordinate the BAA with the underlying services agreement.

g. Include additional term or termination provisions.
h. Authorize termination of the underlying services agreement if the BAA is terminated.
i. Allow for amendment of the BAA as necessary to accommodate changes to the HIPAA Rules.
j. Include choice of law and venue provisions.

Business associates may want to include additional or alternative terms that minimize their exposure, such as:

a. Prohibit covered entities from asking the business associate to take any action that would violate the HIPAA Rules if done by the covered entity.
b. Prohibit covered entities from agreeing to restrictions on the use or disclosure of PHI that might adversely affect the business associate, or notify the business associate of such restrictions.
c. Authorize termination of the BAA if the covered entity agrees to restrictions that materially affect the business associate's ability to perform or costs of performance.
d. Allow the business associate to recover costs associated with such additional restrictions or requirements.
e. Eliminate or limit any insurance or indemnification agreement otherwise requested by the covered entity.
f. Waive or limit damages for which the business associate may be liable under the BAA.

**Liability for Business Associate's Action.** The HIPAA Privacy and Security rules confirm that a covered entity violates HIPAA if the covered entity knew of a pattern of activity or practice of a business associate that constituted a material breach or violation of the BAA unless the covered entity took reasonable steps to cure the breach, end the violation, or terminate the contract. In addition, a covered entity may be vicariously liable for the business associate's misconduct if the business associate was acting as the agent of the covered entity. The same rules apply to a business associates with respect to their subcontractors. Accordingly, covered entities and business associates should ensure that their BAAs:
a. Confirm the business associate or subcontractor is acting as an independent contractor, and not as the agent of the covered entity or business associate; and

b. Confirm that the BAA does not give the covered entity or business associate such control over operational activities so as to make the business associate the agent of the covered entity, or the subcontractor the agent of the business associate.

Effect of No BAA. Covered entities and business associates violate HIPAA if there is no required BAA in place; however, business associates must still comply with the relevant HIPAA Rules even if there is no BAA.

Additional Resources. If you have questions about these or other issues, the Office of Civil Rights maintains a helpful website on HIPAA issues, http://www.hhs.gov/ocr/privacy/. In addition, Holland & Hart has prepared sample HIPAA forms for its clients, including sample business associate and subcontractor agreements. If you are interested in obtaining such forms, please contact me at kcstanger@hollandhart.com.

1 Under HIPAA, "business associates" are generally defined as those entities outside of the covered entity's workforce who create, receive, maintain or transmit PHI on behalf of a covered entity to perform certain enumerated functions, including claims processing; data analysis; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services; data transmission services if routine access to data is required; and subcontractors of business associates. 45 CFR § 160.103.

2 Id. at §§ 164.402 and .404.

3 Id. at §§ 164.308(b) and .502(e)(1)-(2).

4 The Omnibus Rule extends the deadline to September 23, 2014, if (1) the BAA complied with HIPAA rules as they existed before January 25, 2013, and (2) the BAA is not renewed or modified prior to September 23, 2014. See id. at § 164.532(e).

5 Id. at § 164.103.

6 A covered entity need not execute a BAA if the covered entity disclosed only a limited data set (as defined by HIPAA) to the business associate and the covered entity has a data use agreement with the business associate that complies with §§ 164.514(e)(4) and 164.314(a)(1), if applicable. See id. at § 164.504(e)(3)(iv). If the
covered entity and business associate are both governmental entities, the BAA may contain certain alternative or additional provisions. See id. at § 164.504(e)(3).

7Id. at §§ 164.314(a)(2)(iii) and .504(e)(5).

8Id. at § 164.504(e)(2)(i) and (4)(i)-(ii).

9Id. at §§ 164.504(e)(2)(ii) and .314(a)(2)

10Id. at § 164.504(e)(2)(ii)(J) and (iii). The covered entity may omit the provision authorizing termination if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. See id. at § 164.504(e)(3)(iii).

11Id. at § 164.504(e)(1)(ii).

12Id. at § 160.402(c).

13Id. at §§ 160.402(c) and 164.504(e)(1)(iii).

For questions regarding this update, please contact
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

This news update is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author. This news update is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.
Complying With HIPAA: A Checklist for Business Associates

10/26/2015

by Kim Stanger

The HIPAA Privacy, Security, and Breach Notification Rules now apply to both covered entities (e.g., healthcare providers and health plans) and their business associates. A "business associate" is generally a person or entity who "creates, receives, maintains, or transmits" protected health information (PHI) in the course of performing services on behalf of the covered entity (e.g., consultants; management, billing, coding, transcription or marketing companies; information technology contractors; data storage or document destruction companies; data transmission companies or vendors who routinely access PHI; third party administrators; personal health record vendors; lawyers; accountants; and malpractice insurers). With very limited exceptions, a subcontractor or other entity that creates, receives, maintains, or transmits PHI on behalf of a business associate is also a business associate. To determine if you are a business associate, see the attached Business Associate Decision Tree.

Business associates must comply with HIPAA for the following reasons:

1. Civil Penalties Are Mandatory for Willful Neglect. The Office for Civil Rights ("OCR") is required to impose HIPAA penalties if the business associate acted with willful neglect, i.e., with “conscious, intentional failure or reckless indifference to the obligation to comply” with HIPAA requirements. The following chart summarizes the tiered penalty structure:

<table>
<thead>
<tr>
<th>Conduct of covered entity or business associate</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know and, by exercising reasonable diligence, would not have known of the violation</td>
<td>$100 to $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
<tr>
<td>Violation due to reasonable cause and not willful neglect</td>
<td>$1,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
<tr>
<td>Violation due to willful neglect but the</td>
<td>Mandatory fine of $10,000</td>
</tr>
</tbody>
</table>
violation is corrected within 30 days after the covered entity knew or should have known of the violation to $50,000 per violation; Up to $1,500,000 per identical violation per year

Violation due to willful neglect, and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation Mandatory fine of not less than $50,000 per violation; Up to $1,500,000 per identical violation per year

A single action may result in multiple violations. According to HHS, the loss of a laptop containing records of 500 individuals may constitute 500 violations. Similarly, if the violation were based on the failure to implement a required policy or safeguard, each day the covered entity failed to have the required policy or safeguard in place constitutes a separate violation. Not surprisingly, penalties can add up quickly. And the government is serious about the new penalties: the OCR has imposed millions of dollars in penalties or settlements since the mandatory penalties took effect. State attorneys general may also sue for HIPAA violations and recover penalties of $25,000 per violation plus attorneys’ fees. Future regulations will allow affected individuals to recover a portion of any settlement or penalties arising from a HIPAA violation, thereby increasing individuals’ incentive to report HIPAA violations.

The good news is that if the business associate does not act with willful neglect, the OCR may waive or reduce the penalties, depending on the circumstances. More importantly, if the business associate does not act with willful neglect and corrects the violation within 30 days, the OCR may not impose any penalty; timely correction is an affirmative defense. Whether business associates implemented required policies and safeguards is an important consideration in determining whether they acted with willful neglect.

2. HIPAA Violations May Be A Crime. Federal law prohibits any individual from improperly obtaining or disclosing PHI from a covered entity without authorization; violations may result in the following criminal penalties:

<table>
<thead>
<tr>
<th>Prohibited Conduct</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowingly obtaining or disclosing PHI without authorization.</td>
<td>Up to $50,000 fine and one year in prison</td>
</tr>
<tr>
<td>If done under false pretenses.</td>
<td>Up to $100,000 fine and five years in prison</td>
</tr>
<tr>
<td>If done with intent to sell, transfer, or use the PHI for commercial advantage, personal gain or malicious harm.</td>
<td>Up to $250,000 fine and ten years in prison</td>
</tr>
</tbody>
</table>
Physicians, hospital staff members, and others have been prosecuted for improperly accessing, using, or disclosing PHI.

3. Business Associates Must Self-Report HIPAA Breaches. The risk of penalties is compounded by the fact that business associates must self-report HIPAA breaches of unsecured PHI to covered entities, and covered entities must then report the breach to affected individual(s), HHS, and, in certain cases, to the media. The Omnibus Rule modified the Breach Notification Rule to eliminate the former harm analysis; now a breach of PHI is presumed to be reportable unless the covered entity or business associate can demonstrate a low probability that the data has been compromised through an assessment of specified risk factors. Reporting a HIPAA violation is bad enough given the costs of notice, responding to government investigations, and potential penalties, but the consequences for failure to report a known breach are likely worse: if discovered, such a failure would likely constitute willful neglect, thereby subjecting the covered entity or business associate to the mandatory civil penalties.

Given the increased penalties, lowered breach notification standards, and expanded enforcement, it is more important than ever for business associates to comply or, at the very least, document good faith efforts to comply, to avoid a charge of willful neglect, mandatory penalties, and civil lawsuits. The following are key compliance actions that business associates should take.

1. Determine whether business associate rules apply. Out of ignorance or an abundance of caution, covered entities may ask some entities to sign business associate agreements even though the entity is not a “business associate” as defined by HIPAA. Entities should avoid assuming business associate liabilities or entering business associate agreements if they are not truly business associates. Significantly, the following are not business associates: (i) entities that do not create, maintain, use, or disclose PHI in performing services on behalf of the covered entity; (ii) members of the covered entity’s workforce; (iii) other healthcare providers when providing treatment; (iv) members of an organized healthcare arrangement; (v) entities who use PHI while performing services on their own behalf, not on behalf of the covered entity; and (vi) entities that are mere conduits of the PHI. For more information on avoiding business associate agreements, see this link.

2. Execute and comply with valid business associate agreements. Entities that are business associates must execute and perform according to written business associate agreements that essentially require the business associate to maintain the privacy of PHI; limit the business associate’s use or disclosure of PHI to those purposes authorized by the covered entity; and assist covered entities in
responding to individual requests concerning their PHI. The OCR has published sample business associate agreement language on its website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Covered entities may sometimes add terms or impose obligations in business associate agreements that are not required by HIPAA. Business associates should review business associate agreements carefully to ensure they do not unwittingly assume unintended obligations, such as indemnification provisions or requirements to carry insurance. Conversely, business associates may want to add terms to limit their liability, such as liability caps, mutual indemnification, etc. A checklist for business associate agreements and suggested terms is available at this link.

3. Execute valid subcontractor agreements. If the business associate uses subcontractors or other entities to provide any services for the covered entity involving PHI, the business associate must execute business associate agreements with the subcontractors, which agreements must contain terms required by the regulations. The subcontractor becomes a business associate subject to HIPAA. The subcontractor agreement cannot authorize the subcontractor to do anything that the business associate could not do under the original business associate agreement with the covered entity. Thus, business associate obligations are passed downstream to subcontractors. Business associates are not liable for the business associate’s HIPAA violations unless the business associate was aware of a pattern or practice of violations and failed to act, or the subcontractor is the agent of the business associate. To be safe, business associates should confirm that their subcontractors are independent contractors.

4. Comply with privacy rules. Most of the Privacy Rule provisions do not apply directly to business associates, but because business associates cannot use or disclose PHI in a manner contrary to the limits placed on covered entities, business associates will likely need to implement many of the same policies and safeguards that the Privacy Rule mandates for covered entities, including rules governing uses and disclosure of PHI and individual rights concerning their PHI. Those are typically outlined in the business associate’s agreement with the covered entity. Business associates should generally be aware of the Privacy Rule requirements along with any additional limitations or restrictions that the covered entity may have imposed on itself through its notice of privacy practices or agreements with individuals.

The basic privacy rules are relatively simple: covered entities and their business associates may not use, access, or disclose PHI without the
individual’s valid, HIPAA-compliant authorization, unless the use or disclosure fits within an exception. Unless they have agreed otherwise, covered entities and business associates may use or disclose PHI for purposes of treatment, payment or certain health care operations without the individual’s consent. HIPAA contains numerous exceptions that allow disclosures of PHI to the extent another law requires disclosures or for certain public safety and government functions, including: reporting of abuse and neglect, responding to government investigations, or disclosures to avoid a serious and imminent threat to the individual; however, before making disclosures for such purposes, the business associate should consult with the covered entity. Even where disclosure is allowed, business associates must generally limit their requests for or use or disclosure of PHI to the minimum necessary for the intended purpose. The OCR has published a helpful summary of the Privacy Rule:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. (Please note that the summary has not been updated to reflect changes in the Omnibus Rule.)

5. Perform a Security Rule risk analysis. Unlike the Privacy Rule, business associates are directly obligated to comply with the Security Rule. Business associates must conduct and document a risk analysis of their computer and other information systems to identify potential security risks and respond accordingly. HHS has developed and made available a risk assessment tool for covered entities and business associates: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool. In addition, the OCR has published guidance for the risk analysis at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Business associates should periodically review and update their risk analysis. A Massachusetts dermatology practice recently agreed to pay $150,000 for, among other things, failing to conduct an adequate risk assessment of its systems, including the use of USBs.

6. Implement Security Rule safeguards. Like covered entities, business associates must implement the specific administrative, technical and physical safeguards required by the Security Rule. A checklist of the required security rule policies is available here.

7. Adopt written Security Rule policies. As with covered entities, business associates must adopt and maintain the written policies required by the Security Rule. A checklist of required polices is available at this link. According to HHS, maintaining the required written policies is a significant factor in avoiding penalties imposed for “willful neglect.” Rite Aid paid $1,000,000 to settle HIPAA violations based in part on its failure to maintain required HIPAA policies.
8. **Train personnel.** Unlike covered entities, the Privacy and Breach Notification Rules do not affirmatively require business associates to train their workforce members, but the Security Rule does. As a practical matter, business associates will need to train their workforce concerning the HIPAA rules to comply with the business associate agreement and HIPAA regulations. Documenting such training may prevent HIPAA violations and/or avoid allegations of willful neglect if a violation occurs.

9. **Respond immediately to any violation or breach.** The Privacy Rule does not impose any specific requirement on business associates to mitigate violations, but many business associate agreements do. Even if not required by rule or contract, business associates will want to respond immediately to any real or potential violation to mitigate any unauthorized access to PHI and reduce the potential for HIPAA penalties. Prompt action may minimize or negate the risk that the data has been compromised, thereby allowing the covered entity or business associate to avoid self-reporting breaches to the individual or HHS. In addition, as discussed above, a business associate can avoid HIPAA penalties altogether if it does not act with willful neglect and corrects the violation within 30 days.

10. **Timely report security incidents and breaches.** Business associates must notify the covered entity of certain threats to PHI. First, business associates must report breaches of unsecured protected PHI to the covered entity so the covered entity may report the breach to the individual and HHS. Second, the business associate must report uses or disclosures that violate the business associate agreement with the covered entity, which would presumably include uses or disclosures in violation of HIPAA even if not reportable under the breach notification rules. Third, business associates must report “security incidents,” which is defined to include the “attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in a PHI system.”

11. **Maintain Required Documentation.** Business associates must maintain the documents required by the Security Rule for six years from the document’s last effective date. Although not required, documenting other acts in furtherance of compliance may help negate any allegation of willful neglect.

12. **Beware more stringent laws.** In evaluating their compliance, business associates must also consider other federal or state privacy laws. To the extent a state or other federal law is more stringent than HIPAA, business associates should comply with the more restrictive law. In general, a law is more stringent than HIPAA if it offers greater privacy protection to individuals, or grants individuals greater rights regarding their PHI.
CONCLUSION.
Like covered entities, business associates must now comply with HIPAA or face draconian penalties. As many businesses have recently learned, even seemingly minor or isolated security lapses may result in major fines and business costs. Fortunately, business associates may avoid mandatory fines and minimize their HIPAA exposure by taking and documenting the steps outlined above. Business associates may use this outline to evaluate and, where needed, upgrade their overall compliance.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
e mail: kcstanger@hollandhart.com, phone: 208-383-3913

This news update is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author. This news update is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

145 CFR 160.103, definition of “business associate.”
2 Id.; 78 FR 5572.
345 CFR § 160.401 and 164.404.
5See 78 FR 5584 (1/25/13).
6 45 CFR §160.406; 78 F.R. 5584 (1/25/13).
842 USC § 1320d-5(d); See also OCR training for state attorneys general at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html.
9See 78 FR 5568 (1/25/13).
1045 CFR § 160.308(a)(2) and 160.408.
1145 CFR § 160.410.
1342 USC § 1320d-6.
1442 CFR § 164.410.
1545 CFR § 164.400 et seq.
1645 CFR § 164.402; 78 FR 5641 (1/25/13).
1775 FR 40879 (7/14/10).
18 45 CFR § 160.103; 78 FR 5571 (1/25/13).
19 45 CFR § 164.504(e).
20 45 CFR §§ 164.314(a)(2) and 164.504(e)(1).
21 45 CFR § 160.103.
22 45 CFR §§ 164.314(a)(2) and 164.504(e)(5).
23 78 FR 5573 (1/25/13).
24 45 CFR § 164.504(e)(1).
25 45 CFR § 160.402(c).
26 78 FR 5591 (1/25/13).
27 45 CFR § 164.504(e)(2); 78 FR 5591 (1/25/13).
28 See 45 CFR § 164.502(e).
29 45 § CFR 164.502.
30 45 § CFR 164.506.
31 45 § CFR 164.510 and .512.
32 45 CFR § 164.502(b)(1).
33 45 CFR § 164.314(a)(2).
34 45 CFR § 164.308(a)(1).
35 45 CFR §§ 164.306(a), 164.308(a), 164.310, and 164.312.
36 45 CFR § 164.316.
37 45 CFR §§ 164.308(a)(5)
38 45 CFR §§ 160.410.
39 45 CFR § 164.410.
40 45 CFR § 164.504(e)(2).
41 45 CFR § 164.304.
42 45 CFR § 164.316(a)(2).
43 45 CFR § 160.203.
Introduction

The HIPAA Rules regarding electronic health care transactions and the privacy and security of protected health information are regulations issued by the U.S. Department of Health & Human Services (“HHS”) under the authority of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996. The portions of the HIPAA Rules with which this memorandum is concerned are:

- The Privacy Rule, which primarily addresses permitted and prohibited uses and disclosures of protected health information or “PHI”, such as who may have access to an individual’s health information, what they may do with that information, and to whom may they disclose that information;
- The Security Rule, which describes the measures that an organization must take to prevent privacy violations, such as uses or disclosures of information that are prohibited without the written authorization of the individual to whom the information pertains;
- The Data Breach Notification Rule, which describes the circumstances in which individuals, government officials, and certain others must be notified if there is a breach (such as certain an unauthorized uses or disclosures) of unsecured PHI; and
- The Transaction and Code Set Standards, which establish standards for the conduct of certain electronic health care transactions.

Covered Entities and Business Associates

The HIPAA Rules apply to “covered entities” and their “business associates.” “Covered entities” include, broadly speaking, health care clearinghouses (generally, data processors that convert electronic data sets from non-standard formats into standard formats, or vice versa), health plans (such as health insurance issuers, health maintenance organizations or HMOs, and employer-sponsored group health plans), and health care providers that engage in electronic billing and related transactions regulated under the Transaction and Code Set Standards.

---

1 45 C.F.R. Parts 160, 162, and 164.
2 Pub. L. 104-191.
3 45 C.F.R. Part 164, Subpart E.
4 45 C.F.R. Part 164, Subpart C.
5 45 C.F.R. Part 164, Subpart D.
6 45 C.F.R. Part 162.
7 45 C.F.R. § 160.103 (definition of “covered entity”).
Generally speaking, a HIPAA “business associate” is a person or organization that creates, receives, maintains, or transmits PHI in the performance of a function, activity, or service for or on behalf of a covered entity or another business associate.

The HIPAA Rules changed substantially in 2013 with the issuance of amended regulations, commonly known as the “HIPAA Omnibus Rule,” which applied the business associate rules to “subcontractors” of business associates, such as a vendor or other subcontractor to which a business associate has delegated a function, activity, or service that calls for that subcontractor to create, receive, maintain, or transmit PHI on behalf of the business associate. Following this rule change, vendors and others may be subject to regulation under HIPAA as business associates even if they do not do business with HIPAA covered entities directly. So, if an organization’s customer is either a covered entity (such as an employer-sponsored health plan) or a business associate (such as a bank that is the business associate of such a health plan), and that organization creates, receives, maintains, or transmits PHI in the performance of its services for its customer, the organization will be acting as, and will be regulated as, a business associate.9

Regulation of Business Associates & Business Associate Contracts

Business associates are directly regulated under HIPAA by HHS.10 In addition, the HIPAA Rules require covered entities to enter into “business associate contracts” with their business associates, and require that business associates enter into similar business associate contracts with their subcontractors that create, receive, maintain, or transmit PHI in the performance of a function, activity, or service delegated to them by the business associate.11 Business associate contracts generally enumerate key requirements of the HIPAA Rules, and require that the business associate to comply with the HIPAA Rules generally. However, business associates are directly regulated by the HIPAA Rules and are required to comply with the requirements described in this memorandum whether or not they enter into business associate contracts that call for that compliance. Business associate contracts may impose additional obligations upon the business associate in beyond those required by the HIPAA Rules.

---

9 45 C.F.R. § 160.103 (definition of “business associate”); examples of business associate functions include, but are not limited to, claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities, or legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. An individual who performs such functions or services as a member of a covered entity’s or a business associate’s workforce is not a business associate.
10 42 U.S.C. §§ 17931(a) & (b) and 17934(a) & (c), added by the Health Information Technology for Clinical and Economic Health (“HITECH”) Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (“ARRA”), Pub. L. 111-5).
11 45 C.F.R. §§ 164.308(b)(1) & (2), 164.314(a)(1), 164.502(e).
Regulatory Obligations of Business Associates under HIPAA

The following outline provides an overview of the requirements that apply to business associates under the Security Rule, the Breach Notification Rule, the Privacy Rule, and the Transaction and Code Sets Standards. This is a very general summary of these requirements only, and the rules themselves should be consulted for a complete description of the applicable requirements.

I. **General Requirements.** Business associates are required to:
   
   A. **Keep records and submit compliance reports** to the U.S. Secretary of Health and Human Services (“Secretary of HHS”) and **cooperate in complaint investigations and compliance reviews.**\(^\text{12}\)
   
   B. **Give the Secretary of HHS access to facilities, books, records, accounts,** and other information.\(^\text{13}\)

II. **The Security Rule.** Business associates are required to comply with the Security Rule,\(^\text{14}\) which applies to PHI that is in electronic form.\(^\text{15}\)

   A. **General Requirements.** Each business associate is required to do the following:\(^\text{16}\)
      
      1. **Ensure the confidentiality, integrity, and availability** of electronic protected health information (“ePHI”).\(^\text{17}\)
      
      2. **Protect against reasonably anticipated threats or hazards** to the security or integrity of ePHI.\(^\text{18}\)
      
      3. **Protect against reasonably anticipated uses and disclosures of PHI that would violate the Privacy Rule.**\(^\text{19}\)
      
      4. **Ensure compliance by workforce.**\(^\text{20}\)

---

\(^\text{12}\) 45 C.F.R. §§ 160.310(a) 160.310(b).
\(^\text{13}\) 45 C.F.R. § 164.310(c).
\(^\text{14}\) 45 C.F.R. Part 164, Subpart C.
\(^\text{15}\) 45 C.F.R. § 164.302.
\(^\text{16}\) 45 C.F.R. § 164.306.
\(^\text{17}\) 45 C.F.R. § 164.306(a)(1).
\(^\text{18}\) 45 C.F.R. § 164.306(a)(2).
\(^\text{19}\) 45 C.F.R. § 164.306(a)(3); the Privacy Rule is set forth at 45 C.F.R. Part 164, Subpart E.
5. **Comply with Security Rule standards** (listed below).\(^{21}\)

6. **Implement or address “required” and “addressable” “implementation specifications,”** respectively (listed below).\(^{22}\) The Security Rule provides that implementation specifications that are “required” must be implemented and, for implementation specifications that are “addressable,” the business associate must assess whether the specification is reasonable and appropriate in its environment and, if reasonable or appropriate, implement the specification or, if not reasonable and appropriate, document that fact and implement equivalent alternative measures that are reasonable and appropriate. The Rule describes these matters in detail.\(^{23}\)

7. **Maintain, review and modify security measures** as needed.\(^{24}\)

B. **Administrative Safeguards.** The Security Rule requires that a business associate adopt administrative safeguards that include the following:\(^{25}\)

1. Implement a **security management process** through written policies and procedures to prevent, detect, contain, and correct security violations,\(^{26}\) which will include the following:

   a. Conducting an accurate and thorough **risk analysis** assessing potential vulnerabilities to confidentiality, integrity, and availability of ePHI (required).\(^{27}\)

   b. Implementing **risk management** measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level (required).\(^{28}\)

\(^{20}\) 45 C.F.R. § 164.306(a)(4).
\(^{21}\) 45 C.F.R. § 164.306(c).
\(^{22}\) 45 C.F.R. § 164.306(d).
\(^{23}\) 45 C.F.R. § 164.306(d).
\(^{24}\) 45 C.F.R. § 164.306(e).
\(^{25}\) 45 C.F.R. § 164.308.
\(^{26}\) 45 C.F.R. § 164.306(a)(1)(i).
\(^{27}\) 45 C.F.R. § 164.308(a)(1)(ii)(A).
\(^{28}\) 45 C.F.R. § 164.308(a)(1)(ii)(B).
c. Applying an appropriate *workforce sanctions* policy against workforce members who fail to comply with the business associate’s security policies and procedures (required).²⁹

d. Implementing procedures to regularly conduct an *information system activity review* of audit logs, access reports, security incident tracking reports, etc. (required).³⁰

2. Appoint a *security official* who is responsible for the development and implementation of the policies and procedures required for compliance with the Security Rule.³¹

3. Implement *workforce security* policies and procedures,³² which will include the following:

a. Policies and procedures for the *authorization and/or supervision* of workforce members who work with ePHI or in locations where ePHI may be accessed (addressable).³³

b. *Workforce clearance* procedures to determine appropriate access to ePHI for those workforce members (addressable).³⁴

c. *Termination procedures* for terminating those workforce members’ access to ePHI (addressable).³⁵

4. Implement *information access management* policies and procedures for ePHI,³⁶ which will include the following:

a. *Isolating health care clearinghouse functions*, if any (required).³⁷

---

²⁹ 45 C.F.R. § 164.308(a)(1)(ii)(C).
³⁰ 45 C.F.R. § 164.308(a)(1)(ii)(D).
³¹ 45 C.F.R. § 164.308(a)(2).
³² 45 C.F.R. § 164.308(a)(3)(i).
³⁶ 45 C.F.R. § 164.308(a)(4)(i).
b. Implementing **access authorization policies and procedures** for granting access to ePHI through access to a workstation, transaction, program, process, or other mechanism (addressable).\(^{38}\)

c. Implementing **access establishment and modification** policies and procedures to establish, document, review and modify users’ access rights (addressable).\(^{39}\)

5. Implement **security awareness and training** for all workforce members,\(^{40}\) which will include the following:

a. Periodic **security reminders and updates** (addressable).\(^{41}\)

b. Procedures for **protection from malicious software**, including guarding against, detecting, and reporting malicious software (addressable).\(^{42}\)

c. Procedures for **log-in monitoring** and reporting discrepancies (addressable).\(^{43}\)

d. Procedures for **password management**, including creating, changing, and safeguarding passwords (addressable).\(^{44}\)

6. Implement **security incident procedures**,\(^{45}\) which will include **identifying, responding to, and reporting security incidents**, mitigating harmful effects, and documenting those incidents and their outcomes (required).\(^{46}\)

7. Implement a **contingency plan** for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that include ePHI,\(^{47}\) which will include the following:

\(^{38}\) 45 C.F.R. § 164.308(a)(4)(ii)(B).
\(^{39}\) 45 C.F.R. § 164.308(a)(4)(ii)(C).
\(^{40}\) 45 C.F.R. § 164.308(a)(5)(i).
\(^{41}\) 45 C.F.R. § 164.308(a)(5)(ii)(A).
\(^{42}\) 45 C.F.R. § 164.308(a)(5)(ii)(B).
\(^{43}\) 45 C.F.R. § 164.308(a)(5)(ii)(C).
\(^{44}\) 45 C.F.R. § 164.308(a)(5)(ii)(D).
\(^{45}\) 45 C.F.R. § 164.308(a)(6)(i).
\(^{46}\) 45 C.F.R. § 164.308(a)(6)(ii).
a. **A data backup plan** to create and maintain retrievable exact copies of ePHI (required).

b. **A disaster recovery plan** to restore any loss of data (required).

c. **An emergency mode operation plan** to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode (required).

d. **Testing and revision procedures** for periodic testing and revision of contingency plans (addressable).

e. **An applications and data criticality analysis** to assess the relative criticality of specific applications and data in support of other contingency plan components (addressable).

8. Conducting **periodic technical and nontechnical evaluations** to establish the extent to which security policies and procedures meet the Security Rule’s requirements.

9. Entering into appropriate **business associate contracts with subcontractors**.

C. **Physical Safeguards.** The Security Rule requires that a business associate adopt physical safeguards that will include the following:

1. **Facility access controls** to limit physical access to information systems and facilities, including the following:

---

47 45 C.F.R. § 164.308(a)(7)(i).
49 45 C.F.R. § 164.308(a)(7)(ii)(B).
50 45 C.F.R. § 164.308(a)(7)(ii)(C).
51 45 C.F.R. § 164.308(a)(7)(ii)(D).
52 45 C.F.R. § 164.308(a)(7)(ii)(E).
53 45 C.F.R. § 164.308(a)(8).
54 45 C.F.R. § 164.308(b)(2); see also 45 C.F.R. §§ 164.314(a), 164.502(e)(1)(ii), 164.502(e)(2), & 164.504(e)(1).
55 45 C.F.R. § 164.310.
56 45 C.F.R. § 164.310(a)(1).
a. **Contingency operations** procedures that allow facility access in support of the restoration of lost data in the event of an emergency (addressable).\(^\text{57}\)

b. **A facility security plan** to safeguard the facility and equipment from unauthorized physical access (addressable).\(^\text{58}\)

c. **Access control and validation procedures** to control and validate persons’ access to facilities based on their role or function, including visitor, and control of access to software programs for testing and revision (addressable).\(^\text{59}\)

d. **Maintenance records** documenting repairs and modifications to security components, e.g., hardware, walls, doors, and locks (addressable).\(^\text{60}\)

2. Policies and procedures for **proper workstation use**.\(^\text{61}\)

3. Physical safeguards for **workstation security**, to restrict access to ePHI by authorized users.\(^\text{62}\)

4. Policies and procedures for **device and media controls** to govern receipt and removal from the facility of hardware and electronic media containing ePHI and the movement of those items within the facility,\(^\text{63}\) including the following:

   a. **Disposal** of ePHI and/or hardware or electronic media on which it is stored (required).\(^\text{64}\)

   b. **Media re-use**, to address removal of ePHI from electronic media before it is made available for re-use (required).\(^\text{65}\)

---

\(^{57}\) 45 C.F.R. § 164.310(a)(2)(i).
\(^{58}\) 45 C.F.R. § 164.310(a)(2)(ii).
\(^{59}\) 45 C.F.R. § 164.310(a)(2)(iii).
\(^{60}\) 45 C.F.R. § 164.310(a)(2)(iv).
\(^{61}\) 45 C.F.R. § 164.310(b).
\(^{62}\) 45 C.F.R. § 164.310(c).
\(^{63}\) 45 C.F.R. § 164.310(d)(1).
\(^{64}\) 45 C.F.R. § 164.310(d)(2)(i).
c. **Accountability** for movement of hardware and electronic media, by documenting movements of hardware and media and the persons responsible therefor (addressable).  

66

d. **Data backup and storage**, to create a retrievable, exact copy of ePHI when needed, before the movement of equipment (addressable).  

57

D. **Technical Safeguards.** The Security Rule requires that a business associate adopt technical safeguards that include the following:  

68

1. Policies and procedures for **access control** to allow access to electronic information systems that maintain ePHI only by those persons or software programs that have been granted access rights, including the following:  

   a. **Unique user identification** (required).  

   70

   b. **Emergency access procedures** (required).  

   71

   c. **Automatic logoff** after predetermined period of inactivity (addressable).  

   72

   d. **Encryption and decryption** of ePHI (addressable).  

   73

2. **Audit controls** for hardware, software, and/or procedural mechanisms.  

74

3. Policies and procedures to maintain **data integrity**, to protect ePHI from improper alteration or destruction, including a mechanism to

---

65 45 C.F.R. § 164.310(d)(2)(ii).
68 45 C.F.R. § 164.312.
69 45 C.F.R. § 164.312(a)(1).
70 45 C.F.R. § 164.312(a)(2)(i).
71 45 C.F.R. § 164.312(a)(2)(ii).
72 45 C.F.R. § 164.312(a)(2)(iii).
73 45 C.F.R. § 164.312(a)(2)(iv).
74 45 C.F.R. § 164.312(b).
75 45 C.F.R. § 164.312(c)(1).
authenticate ePHI to corroborate that ePHI has not been altered or destroyed in an unauthorized manner (addressable).76

4. Procedures for person or entity authentication to verify that a person or entity seeking access to ePHI is the one claimed.77

5. Technical measures for transmission security to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network,78 including the following:

a. Integrity controls to ensure that electronically transmitted ePHI is not improperly modified without detection (addressable).79

b. A mechanism for encryption of ePHI whenever deemed appropriate (addressable).80

E. Organizational Requirements. The Security Rule requires that a business associate enter into appropriate business associate contracts with subcontractors:81

F. Documentation Requirements. The Security Rule requires that a business associate comply with the following documentation requirements:82

1. Maintain reasonable and appropriate policies and procedures to comply with Security Rule,83 taking into account the business associate’s size, complexity, and capabilities; its technical infrastructure, hardware and software capabilities; the costs of security measures; and the probability and criticality of potential risks to ePHI.84

---

76 45 C.F.R. § 164.312(c)(2).
77 45 C.F.R. § 164.312(d).
78 45 C.F.R. § 164.312(c)(1).
79 45 C.F.R. § 164.312(e)(2)(i).
80 45 C.F.R. § 164.312(e)(2)(ii).
81 45 C.F.R. § 164.314(a); see also 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), 164.502(e)(2), & 164.504(e).
82 45 C.F.R. § 164.316.
83 45 C.F.R. § 164.316(a).
84 45 C.F.R. § 164.306(b)(2).
2. **Document required actions, activities, and assessments** to create a record of compliance with the Security Rule,\(^8^5\) and comply with the following standards:

   a. Retain documentation for **six (6) year time limit** (required).\(^8^6\)

   b. **Make documentation available** to persons responsible for compliance (required).\(^8^7\)

   c. Periodically **review and update** documentation as needed in response to environmental or operational changes affecting the security of ePHI (required).\(^8^8\)

III. **The Breach Notification Rule.** Business associates are required to comply with specified provisions of the Breach Notification Rule,\(^8^9\) including the following:\(^9^0\)

   A. **Notify the covered entity** of a breach of unsecured PHI\(^9^1\) without unreasonable delay and in no case later than sixty (60) days following the breach.\(^9^2\) Often, business associate contracts reduce the period of time within which these reports are required to be made.

   B. **Provide specified information** to the covered entity.\(^9^3\)

   C. Often, business associate contracts impose additional requirements in connection with data breach reporting.

IV. **The Privacy Rule.** Business associates are required to comply with specified provisions of the Privacy Rule,\(^9^4\) which requires that a business associate do the following:\(^9^5\)

---

\(^8^5\) 45 C.F.R. § 164.316(b)(1).
\(^8^6\) 45 C.F.R. § 164.316(b)(2)(i).
\(^8^7\) 45 C.F.R. § 164.316(b)(2)(ii).
\(^8^8\) 45 C.F.R. § 164.316(b)(2)(iii).
\(^8^9\) 45 C.F.R. Part 164, Subpart D.
\(^9^0\) 45 C.F.R. § 164.410.
\(^9^1\) 45 C.F.R. § 164.410(a).
\(^9^2\) 45 C.F.R. § 164.410(b).
\(^9^3\) 45 C.F.R. § 164.410(c).
\(^9^4\) 45 C.F.R. Part 164, Subpart E.
\(^9^5\) 45 C.F.R. § 164.500(c).
A. **Use and disclose PHI only as permitted** or required by the applicable business associate contract or as required by law.\(^{96}\)

B. **Disclose PHI to Secretary of HHS** when required.\(^{97}\)

C. **Disclose PHI to covered entity or individual** when necessary to provide for individuals to have the access to their PHI for which HIPAA provides.\(^{98}\)

D. **Refrain from selling PHI** unless exception to rule applies.\(^{99}\)

E. Make reasonable efforts to limit the use, disclosure, or requests for PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure or request.\(^{100}\)

F. Disclose PHI to a subcontractor, and permit that subcontractor to create, receive, maintain, or transmit PHI on the business associate’s behalf, only if the business associate **obtains satisfactory assurances that the subcontractor will appropriately safeguard the PHI**; in other words, a business associate must enter into business associate contracts with those subcontractors.\(^{101}\)

G. **Comply with business associate contracts** with covered entities (and business associates to which the business associate is a subcontractor), including the following: \(^{102}\)

1. **Not use or disclose PHI in a way that would violate the Privacy Rule if done by the covered entity.** \(^{103}\)

2. **Not use or disclose PHI other than as permitted or required by the business associate contract or as required by law.** \(^{104}\)

\(^{96}\) 45 C.F.R. § 164.502(a)(3).

\(^{97}\) 45 C.F.R. § 164.502(a)(4)(i).

\(^{98}\) 45 C.F.R. § 164.502(a)(4)(ii); see 45 C.F.R. § 164.524(c).


\(^{100}\) 45 C.F.R. § 164.502(b).

\(^{101}\) 45 C.F.R. § 164.502(e)(1)(ii); see also 45 C.F.R. §§ 164.308(b)(2), 164.314(a), & 164.502(e)(2).

\(^{102}\) Note that this requires the business associate to be familiar with all the Privacy Rule’s requirements, even if those requirements do not apply to the business associate directly.

\(^{103}\) 45 C.F.R. § 164.504(e)(2)(i).

\(^{104}\) 45 C.F.R. § 164.504(e)(2)(ii)(A).
3. **Comply with the Security Rule.**\(^{105}\)

4. **Report unauthorized uses or disclosures, security incidents, and breaches of unsecured PHI, to the covered entity.**\(^{106}\)

5. **Ensure that subcontractors agree to same restrictions and conditions that apply to business associate with respect to PHI.**\(^{107}\)

6. **Make PHI available as needed comply with individuals’ rights of access to their PHI.**\(^{108}\)

7. **Make PHI available for amendment and incorporate amendments required under HIPAA or agreed to by the covered entity.**\(^{109}\)

8. **Make information available for required accountings of disclosures of PHI.**\(^{110}\)

9. **If the business associate carries out the covered entity’s obligations under the Privacy Rule, do so in compliance with the Privacy Rule.**\(^{111}\)

10. **Make practices, books, and records available to the Secretary of HHS for compliance review.**\(^{112}\)

11. **Return or destroy PHI at end of the contract, if feasible.**\(^{113}\)

12. Other obligations that may optionally be specified in the business associate contract.\(^{114}\)

---


\(^{107}\) 45 C.F.R. § 164.504(e)(2)(ii)(D).


\(^{110}\) 45 C.F.R. § 164.504(e)(2)(ii)(G) & 164.528.

\(^{111}\) 45 C.F.R. § 164.504(e)(2)(ii)(H).

\(^{112}\) 45 C.F.R. § 164.504(e)(2)(ii)(I).

\(^{113}\) 45 C.F.R. § 164.504(e)(2)(ii)(J).

\(^{114}\) See, e.g., 45 C.F.R. § 164.504(e)(4).
H. Manage relationships with subcontractors appropriately, including the following:

1. *Enter into business associate contracts with subcontractors.*\(^{115}\)

2. *Ensure that subcontractors agree to same restrictions and conditions* that apply to business associate with respect to PHI.\(^{116}\)

3. *Respond to subcontractors’ material breaches* of their business associate contracts, by terminating, if feasible, those subcontracts if reasonable steps to cure those breaches are unsuccessful.\(^{117}\)

V. **Transaction and Code Set Standards.** If a business associate conducts standard transactions (i.e., electronic health care transactions subject to the Transaction and Code Set Standards) on behalf of covered entities:

A. *Use National Provider Identifiers (“NPIs”) and Health Plan Identifiers (“HPIDs”) appropriately.*\(^{118}\)

B. *Comply with applicable Transaction and Code Set Standards, and require subcontractors to do the same.*\(^{119}\)

\(^{115}\) 45 C.F.R. §§ 164.314(a)(2)(i)(B) & 164.504(e)(5).

\(^{116}\) 45 C.F.R. § 164.504(e)(2)(ii)(D).

\(^{117}\) 45 C.F.R. § 164.504(e)(1)(iii).

\(^{118}\) 45 C.F.R. §§ 162.410(a)(5) & 162.510(b).

\(^{119}\) 45 C.F.R. §§ 162.923(c).