Managing Information Privacy & Security in Healthcare

Business Associates[1]

By Barbara Demster, MS, RHIA, CHCQM and Gary L. Kurtz, CHPS, FHIMSS

Overview

A business associate as defined by HIPAA is a person or entity who: (1) on behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates (other than in the capacity of a member of the workforce of such covered entity or arrangement) creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (2) provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected ~~individually identifiable~~ health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

The HIPAA Privacy Rule at §164.502(e)(1) addresses conditions for disclosure of protected health information to business associates. According to §164.502(e)(1)(i), a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. However, a covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

§ 164.502(e)(1)(ii) provides that a business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive,

[1] Updated to include HIPAA Omnibus Rule amendments (78 FR 5566 (January 25, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf). Underlined text indicates amendments in view of the Omnibus Rule and text which has been struck through indicates redactions in view of the Omnibus Rule. Blue font indicates actual text from the respective rules.

© Healthcare Information and Management Systems Society.

maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances in accordance with 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

According to §164.502(e)(2), satisfactory assurances must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).

Identifying a Business Associate Under HIPAA

Who is a "business associate" under HIPAA? It is not always a black and white decision. It is also possible for one person or entity to wear several hats. A Medical Director or Pharmacist may be hired to perform administrative functions for a covered entity in which case they would be considered Business Associates and require a Business Associate Agreement. They may also function in a role of provider providing treatment which exempts them from being a business associate and therefore no business associate contract is required.

Let's first start by understanding how the HIPAA Omnibus Rule defines a "business associate" (§160.103). A "business associate" is a person who, on behalf of a covered entity or of an organized health care arrangement which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing, or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

A "business associate" (§160.103) specifically includes: (i) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information; (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity; and (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

However, a "business associate does not include: (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual; (ii) a plan sponsor. with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor. To the extent that the requirements of § 164.504(f) of this subchapter apply and are met; (iii) a government agency, with respect to determining eligibility for, or enrollment in, a government health plan that

© Healthcare Information and Management Systems Society.

provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law; or (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

The AHIMA article "Identifying Your Business Associates Under HIPAA Privacy Regulations" <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok3_005270.hcsp> describes the process for identifying business associates and speaks to inventory of business relationships, definitions to determine who qualifies as a business associate, and amending contracts of existing business partners who now qualify as business associates and not just simple suppliers or vendors. The document "Guidelines for Determining Business Associate Agreements" <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_024583.pdf> provides an orderly decision tree process for determining whether or not a person or entity is to be considered a business associate. Once that determination is made, a business associate contract will be required containing the obligations of the business associate.

Business Associate Contracts

The HHS web page on "Sample Business Associate Agreement Provisions" <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html> details the content of a Business Associate Agreement (BAA). It describes what must be included in the document and notes that contracts between business associates and business associates that are subcontractors are subject to the same requirements.

While there are many boilerplate business associate agreements, they must be carefully reviewed by both parties to ensure that their specific relationship is adequately covered. While many may be routine and repetitive, there are those special relationships where greater care must be taken in drafting the agreements. Those situations arise with the handling of PHI relating to alcohol and drug, genetic, and HIV related activities. More stringent state and federal laws and regulations may require more attention to the detail of the contract. The article "Special Considerations for Business Associate Agreements: Substance Abuse Treatment, Federal Law Present Challenges" <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022663.hcsp> discusses the special issues involved in relationships where there is a higher level of protection expectation for PHI.

Obligations of Business Associates

The HIPAA Privacy Rule at §164.504(e)(2)(ii) requires that the business associate agree in the contract to the following obligations:

(A) Not use or further disclose the PHI other than as permitted or required by the contract or as required by law.

© Healthcare Information and Management Systems Society.

(B) Use appropriate administrative, physical and technical safeguards and comply, where applicable with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by the contract. The sample Business Associate Agreement includes examples of basic safeguard expectations. The HIPAA Security Rule also requires incorporation of these same controls in business associate agreements. Examples of basic security safeguards to include in a contract are:

1. Maintain appropriate clearance procedures and provide supervision to assure that its workforce follows security procedures;

2. Notify the covered entity's Security Officer of the termination or reassignment of any of its workforce members that has access to the covered entity's network, servers, applications, or other resources;

3. Identify and document the termination procedures required for removing any workforce member's access from the covered entity's network, servers, applications, or other resources;

4. Provide appropriate training for the business associate's workforce members to assure compliance with its security policies.

5. Implement appropriate security incident procedures and provide training to its workforce members sufficient to detect, identify, handle, and respond to security incidents. Procedures should include mitigation, to the extent practicable, of any harmful effect that is known to or otherwise discovered by the business associate of a use or disclosure of protected health information in violation of the requirements of the agreement;

6. Maintain a current contingency plan in case of an emergency;

7. If appropriate, maintain an emergency access plan to assure that the protected health information it holds on behalf of the covered entity is available when needed;

8. Implement appropriate storage, disposal and reuse procedures to protect any protected health information that the business associate holds for the covered entity;

9. Provide appropriate backup of the protected health information that it holds for the covered entity;

10. Have in place appropriate authentication and access controls to safeguard the protected health information that the business associate holds for the covered entity;

11. Make use of appropriate encryption for data at rest (e.g., stored or archived PHI) and data in motion (e.g., transmitting PHI over a network);

12. Retain the documentation required by this agreement for six years from the date of its creation or the date when it last was in effect, whichever is later.

© Healthcare Information and Management Systems Society.

(C) Report to the covered entity any use or disclosure of the information not provided for by the contract of which it becomes aware, including breaches of unsecured protected health information as required by §164.410;

(D) In accordance with §164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information, and to implement reasonable and appropriate safeguards to protect it;

(E) Make available protected health information in accordance with the right of access standard in §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation;

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary[2] for purposes of determining the covered entity's compliance with this subpart; and

The HIPAA Privacy Rule at §164.504(e)(2)(iii) requires that, with respect to the business associate agreement, at termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Accounting of Disclosures

Section 164.528 of the HIPAA Privacy Rule addresses accounting of disclosures of protected health information. The standard establishes the individual's right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested.

The covered entity must provide the individual with a written accounting that meets the requirements as defined in the regulation. Section 164.528(b)(1) goes on to state that the

[2] This means the U.S. Secretary of the Department of Health and Human Services.

© Healthcare Information and Management Systems Society.

accounting must include disclosures of protected health information that occurred no more than six years (or shorter time period as requested by the individual) prior to the date of the request for an accounting and that the accounting must include disclosures to or by a business associate of the covered entity.

Section 164.528(b) of the rule requires the covered entity to produce the report of disclosures to the individual. This means that the covered entity must incorporate into their report all qualifying disclosures made by all of their business associates.

Three critical issues with the disclosure reporting by the business associate to the covered entity is defining what, how, and when to report. Unsuccessful security breaches are a major problem in deciding what to report. It is not uncommon for major centers to have their servers "pinged" hundreds of times a day. The usefulness of this information to the covered entity or to the individual requesting an accounting is questionable at best. It is important for the covered entity and the business associate to define in their Business Associate Agreement the types of security incidents they consider important to report. Some covered entities insert the phrase "successful security breaches" to indicate the level of reporting.

Timeliness of reporting must be agreed upon so that the covered entity can meet their response time obligations to the individual. Adequate documentation of disclosures must be maintained both by the covered entity and the business associate. The covered entity will want to ensure that the business associates maintain their disclosures documentation for an appropriate period of time.

While the covered entity is required to maintain at least six years on hand, the business associate may opt to discard their documentation on a much shorter timeframe after fulfilling their obligation to report to the covered entity. The covered entity may want to ensure in writing the length of time that the business associate will retain this documentation. The business associate and the covered entity should have persons designated to coordinate this activity. This is usually handled by the privacy, security, and/or compliance officers of the respective organizations.

This summary only addresses accounting of disclosures as it applies to business associates. The detailed content of the accounting is defined in Section 164.528(b)(2) through 164.528(b)(4).

Breach of Confidentiality by Business Associate

The covered entity may terminate the Business Associate Agreement and the underlying business relationship if it suspects that the business associate has improperly used or disclosed the covered entity's protected health information.

If a business associate breaches its obligations under its agreement with the covered entity, the covered entity must make an effort to mitigate any untoward fallout from the breach. The covered entity may require the business associate to:

1. Provide copies of its practices, procedures, books and records to facilitate mitigation of damages arising from any improper use or disclosure of protected health information.
2. Exercise all reasonable efforts to retrieve improperly used or disclosed protected health

© Healthcare Information and Management Systems Society.

information.

3. Establish and adopt new practices, policies, and procedures to ensure that the protected health information is not used or disclosed in the future in violation of the Business Associate Agreement.
4. Comply with all auditing or reporting requests by the covered entity to demonstrate their compliance with the business associate agreement.
5. Take any other action that the covered entity may reasonably require to mitigate the situation.
6. Terminate the business associate agreement and, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information (§164.504(e)(2)(iii)). However, 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 §164.504(e)(2)(iii).

Disposition of Protected Health Information Upon Termination of Contract

Section 164.504(e)(2)(iii) of the HIPAA Privacy Rule addresses disposition of protected health information upon termination of the business associate relationship. Termination may be for cause (breach of contract) or for other legitimate business reasons. The rule requires that, if feasible, all protected health information in the possession of the business associate be either returned to the covered entity or destroyed, that protected health information in any form must be returned or destroyed, and no copies of protected health information may be retained by the business associate.

If circumstances are such that it is clearly not feasible to return or destroy the protected health information, then the protections of the contract or business associate agreement must be extended to cover the protected health information for its lifetime. Provisions limiting further use and disclosure of the protected health information by the business associate should be addressed in the business associate agreement.

Sample Documents

a. Sample Business Associate Policy

b. Sample Business Associate Agreement (BAA)

c. Cover Letter from Covered Entity to Business Associate

© Healthcare Information and Management Systems Society.