

HIPAA PRIVACY RULES –

**WHAT IS IT WITH THESE
BUSINESS ASSOCIATES?**

HIPAA PRIVACY RULES–WHAT IS IT WITH THESE BUSINESS ASSOCIATES?

Julie Neerken
Rodey, Dickason, Sloan, Akin & Robb, P.A.
(505) 766-7557
jpneerke@rodey.com

1. Determining Who Are Business Associates

Covered entities need to determine who are their business associates, and whether any exceptions to the requirement of a written agreement apply. Not everyone with whom a covered entity associates is a business associate under HIPAA. In fact, not everyone a covered entity gives PHI to is a business associate. The business associate rule applies when the contract generating the contact with PHI is for services performed for the covered entity. If the business is acting independently or on behalf of someone other than the covered entity, there is no HIPAA business relation. An example: physicians who contract with a health plan to be on its panel are not business associates of the health plan. The U.S. Postal Service and UPS are not business associates.

The regulations define “business associate” as a person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity’s work force. A business associate can also be a covered entity

in its right. A business associate is neither a covered entity nor a work force member. A work force member is someone who is an employee, volunteer, trainee, or other person whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not paid by the covered entity.

Dealing with HIPAA's business associate requirements is a four step process. Step one is deciding who is a business associate. A business associate is an entity or individual who performs or assists in the performance by a covered entity of :

1. A function or activity involving the use or disclosure of individually identifiable health information (including claims processing or administration, data analysis, quality assurance, billing, and benefits management); and
2. A function or activity regulated by HIPAA. 45 CFR 160.103.

A business associate provides, other than in the capacity of a member of the workforce of the covered entity, legal, actuarial, accounting, consulting, data aggregation, management,

administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from the covered entity or arrangement, or from another business associate of the covered entity or arrangement. Another covered entity may be a business associate in specific situations (such as where a doctor is providing staff training for a hospital). Accrediting organizations are business associates.

Often, non-covered entities will have interest in protected health information. For example, workers' compensation carriers, property, casualty, life and disability insurers, re-insurers and stop loss carriers may want the same type of information. The regulation permits disclosure of protected health information without authorization if the disclosure is required by law. 45 CFR 164.512. In addition, certain activities carried on by reinsurers and stop-loss carriers are "healthcare operations", so that when engaged in such activities, such carriers may receive protected health information without authorization.

There are entities that fall into exceptions from business associates' round-up.

1. Work Force. Members of the covered entity's work force are not that entity's business associates. The work force includes employees, volunteers, trainees, and anyone else whose performance of work for the covered entity is under that entity's direct control, whether or not the covered entity is paying for the work.

2. Treatment. The covered entity need not enter into a business associate agreement with a healthcare provider with which or whom it shares PHI if the provider's sole activity is treating patients.

3. Disclosures Between a Group Health Plan and Plan Sponsor. The business associate rules do not apply to disclosures by a group health plan to a plan sponsor. These disclosures must conform to requirements under Regulation Section 164.504(f) of the privacy rules.

4. Organized Healthcare Arrangements. Providers that participate in an organized healthcare arrangement are not business associates of one another. The HIPAA privacy standards apply to more than

one type of organized healthcare arrangement, the first being a clinically integrated setting in which patients receive care from multiple providers. In addition, group health plans may form organized healthcare arrangements, such as a group health plan and a health insurer or HMO (with respect to the PHI of participants or beneficiaries, created or received by the issuer HMO); multiple group health plans maintained by the same plan sponsor; or multiple group health plans maintained by the same plan sponsor and a health insurance issuer or HMO (with respect to the PHI of participants or beneficiaries, created or received by the issuer or HMO).

5. Limited Data Sets. A limited data set is PHI that excludes certain direct identifiers, such as names, social security numbers, and electronic e-mail addresses, but is not completely de-identified in accordance with the HIPAA requirements. The sharing of de-identified information does not require a business associate contract, and does not involve PHI. If a covered entity contracts for services with another party under an arrangement that involves the use and disclosure of information in a limited data set, no business contract is required. Instead, the parties must enter into a data use

agreement which contains similar privacy protections but is not the same as a business associate contract.

2. Examine Business Associate Contracts For HIPAA Compliance

Step two is to look at the documentation in place. Business associate contracts should have the required provisions. Under the privacy regulation, the contract between a covered entity and its business associates must:

- (a) establish the permitted and required uses and disclosures of information by the business associate;
- (b) not authorize the business associate to use or further disclose the information in a manner that would violate the privacy regulations if done by the covered entity;
- (c) require the business associate to not use or further disclose the information other than as permitted by the contract or law;
- (d) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract;

- (e) report to the covered entity any use or disclosure of the information not provided for by the contract of which a business associate becomes aware;
- (f) require that any agents, including subcontractors, to whom the business associate provides protected health information from the covered entity, agree to the same restrictions and conditions that apply to the business associate with respect to the information;
- (g) make available protected health information in accordance with the portion of the privacy regulation on access of individuals to protected health information;
- (h) make available the information required to provide an accounting of disclosures in accordance with the regulations;
- (i) make its internal practices, books, and records relating to the use and disclosure of protected health information received from, created or received by the business associate on behalf of the covered entity, available to HHS for purposes of verifying compliance;

- (j) at the termination of the contract, if feasible, require the return or destruction of 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 preclude retention of copies of such information, or, if the return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to the purposes that made the return or destruction of the information not feasible; and

- (k) authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

The privacy rules provide transition provisions for existing contracts with business associates. Covered entities with business associate contracts in place prior to October 15, 2002 may continue to operate under those contracts until April 14, 2004 even though the contents do not contain the required elements as long as the contracts are not renewed or modified. “Evergreen” or automatically renewing contracts are also eligible for this extension. But if the covered entity uses this transition provision, the covered entity must secure its

business associates' cooperation in implementing the rights of access and amendment.

Business associate contracts in plan should be reviewed for compliance with a number of the covered entity's duties. A covered entity has a duty to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of the covered entity's policies and procedures or the requirement of the privacy regulation by either the covered entity or its business associate. This may require the covered entity to demand that a business associate change its practices. Otherwise, the covered entity may need to terminate the relationship. Bear in mind that if the covered entity is an ERISA fiduciary, this duty takes on fiduciary colors. The contract should reflect this.

A covered entity must demand that the business associate agree to keep documentation for six years from the date of the creation or the date when it was last in effect and to either return it or destroy it upon completion of the contract. Again, if the covered entity is a group health plan under ERISA, ERISA will affect this duty. Like HIPAA, ERISA has record retention requirements (ERISA Section 107), but subject to a fiduciary standard, and if the covered entity has the business associate/TPA keep most of the documentation, the covered entity will

want to require the third party administrator to deliver the documentation to the covered entity, rather than to destroy it, when the contract terminates.

3. Terms of Business Associate Agreements

Third, the terms (including the required terms above) need to be incorporated in a written agreement. HHS has a model business associate agreement; it is at the end of this chapter. Many covered entities use the model business associate agreement as a beginning point.

There are a number of items, in addition to those addressed in the model business associate agreement, that contracting parties will want to put in such an agreement, and some provisions that one contracting party may want to put in, and the other may feel are inappropriate.

It is in the interest of both parties to have in language providing that there will be no third party beneficiary of the contract, to avoid unnecessary exposure to third parties. Covered entities may want to require authorization before a business associate can enter into any subcontracts involving that covered entity's PHI. Alternatively, it may be in both parties' interests to set forth subcontracting guidelines, providing details on how the privacy regulations would be applied

when subcontracting is done by the business associate. Both parties should be clear on who will be dealing with requests for amendment of PHI: covered entities may not want individuals (participants or patients) dealing directly with a business associate.

In addition, the covered entity may wish to have an audit provision, which permits the covered entity to audit the business associate's privacy policies and procedures, or perhaps a provision requiring a periodic audit by a third party selected by the covered entity.

Most problematic may be an indemnification clause, so that the covered entity is indemnified for any expense or loss (including the ever-present attorneys' fees) for privacy compliance violations. The business associate may, on the other hand, feel that there is no need for an additional indemnification, and any other indemnifications which may exist by operation of other contractual commitments are sufficient. Many covered entities will feel that the business associate is an expert in the area, and that the business associate has managed to secure the contract with the covered entity through the business associate's representations of expertise in the area, and it is fair to expect the business associate to stand behind his or her work.

Another problematic provision is one requiring the business associate to provide HIPAA services without additional charge. This issue may be raised for routine services and with respect to complaints with respect to the handling of PHI. The covered entity may feel that this is no more than requiring the business associate to provide what it already contracted to provide and to stand behind its work; the business associate may feel that this is a new and rapidly developing field requiring additional steps in providing services and where no one can anticipate all contingencies, and that the business associate has the right to be paid for all its work. And costs of PHI destruction or return upon contract termination should be addressed currently, rather than when the contract is ending.

4. Avoid Unnecessary Business Associate Contracts

If an entity is not a business associate, such as where the entity is not acting on behalf of a covered entity, the covered entity should not enter into a business associate contract with the entity. Such a contract would burden both parties with provisions not appropriate to their relationship, such as that the entity return or destroy information. In the long run, having a business associate contract where none is needed will add unneeded expense and paperwork.

5. Review Existing Business Associate Contracts to Determine the Effect of the Transition Period.

As indicated above, some will require amendment because of their terms, and some will qualify for the extension until April 14, 2004. However, most covered entities will want to address the requirements sooner rather than later.

Addressing requirements now will make it certain that the business associate is able to provide the required information for individuals' access to their own PHI – and there is no extension on that requirement.

The business associates issues under HIPAA will be issues covered entities will want to address immediately, and which will likely be a source of continued review in the foreseeable future.

MEDICAL PRIVACY - NATIONAL STANDARDS TO PROTECT THE PRIVACY OF PERSONAL HEALTH INFORMATION

a. SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language.

These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule.

The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for

compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions¹

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

- b. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].
- c. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
- d. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- e. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- f. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- g. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

h. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

- i. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- j. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- k. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
- l. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

- m. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

- n. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

- o. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

- p. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- q. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
- r. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

s. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

[List Purposes].

t. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

- u. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- v. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- w. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).

- x. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

- y. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- z. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- aa. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such

restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

bb. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

cc. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- . Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
- . Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
- . If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

d. Effect of Termination.

. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

- c. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- d. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- e. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
- f. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

¹ Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

The HIPAA final regulation can be found at

<http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm>

and the preamble to the final regulation is at

<http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm>

The final HIPAA Security regulation is at:

<http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm>

221482