

## WHO IS A BUSINESS ASSOCIATE?

### Examples of entities that may be Business Associates

This is not an all inclusive list. See the definition if you have doubts.

Collection Agency  
Accountant (If you give the accountant PHI)  
Attorney (If they receive PHI from you)  
Transcriptionist  
Technology and System companies or individuals (if they can access your records)  
Companies that produce patient bills  
Companies that store or retrieve files for the practice  
Shredding Companies  
Personal Health Record companies  
EPrescribing Gateways  
Transmission companies if they access your information  
Companies that might have your backup data storage  
Companies that make appointment reminder calls or handle after hours phone calls  
Patient Safety Organizations  
Health Information Organizations

### Companies that are not BAs.

Cleaning companies (They do not use PHI to do their job)  
Labs (They are part of the treatment chain and are exempt)  
Financial companies if all they do is process deposits or payments for you.  
Other healthcare providers in the treatment cycle.

*The information below on Business Associates has been obtained from various documents produced by Health and Human Services (HHS) from 2002-2010. The documents include the HIPAA regulations, HHS Guidance document of 2002, 2005 & 2010, the NPRM on comments and decisions by HHS, HHS Q&A on their web site, OCR rulings on complaints received from patients that set a precedent for future rulings, the 2009 Stimulus Bill, the FTC Red Flag Rules, the HITECH Act and HHS regulations published as required by HITECH. This information is provided to assist practices in making decisions on who is and is not a business associate, the responsibility of the practice for the actions of Business Associate and information on the need for and purpose of a contract.*

### July 2010 NPRM § 160.103 Definitions.

**Business associate:** (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of protected health information, 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

(B) Any other function or activity regulated by this subchapter; or (ii) 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.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* 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. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *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 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. (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.

### **§ 160.103 Definitions (2005)**

*Business associate*: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of protected health information, 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

(B) Any other function or activity regulated by this subchapter; or

(ii) 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.

(2) A covered entity may be a business associate of another covered entity.

**(3) Business associate includes: (New from the HITECH Act)**

- (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.
- (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

**HHS Response to Comments Received from Original Rulemaking  
Business Associate Contracts**

**Software vendors are business associates** if they perform functions or activities on behalf of, or provide specified services to, a covered entity. The mere provision of software to a covered entity would not appear to give rise to a business associate relationship, although if the vendor needs access to the protected health information of the covered entity to assist with data management or to perform functions or activities on the covered entity's behalf, the vendor would be a business associate. We note that when an employee of a contractor, like a software or IT 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. See the preamble discussion to the definition of workforce, § 160.103.

The Privacy Rule explicitly defines **organizations that accredit covered entities** as business associates. See the definition of "business associate" at § 160.103. The Department defined such organizations as business associates because, like other business associates, they provide a service to the covered entity during which much protected health information is shared.

With regard to **medical device manufacturers**, we clarify that a device manufacturer that provides "health care" consistent with the rule's definition, including **being a "supplier" under the Medicare** program, is a health care provider under the final rule. We do not require a business associate contract when protected health information is shared among health care providers for treatment purposes. However, a device manufacturer that does not provide "health care" must be a business associate of a covered entity if that manufacturer receives or creates protected health information in the performance of functions or activities on behalf of, or the provision of specified services to, a covered entity.

Disclosures from a covered entity to a **researcher for research purposes** as permitted by the Rule do **not require a business associate contract**.

However, the Department does not believe that it is appropriate to exempt attorneys from the business associate requirements.

*Response:* We design the rule's requirements with respect to volunteers and pro bono services to allow flexibility to the covered entity so as not to disturb these arrangements. Specifically, when such **volunteers work on the premises of the covered entity, the covered entity may choose to treat them as members of the covered entity's workforce or as business associates**. See the definitions of business associate and workforce in § 160.103. If the volunteer performs its work off-site and needs protected health information, a business associate arrangement will be required. In this instance, **where protected health information leaves the premises of the covered entity, privacy concerns are heightened and it is reasonable to require an agreement to protect the information**. We believe that pro bono contractors will easily develop standard contracts to allow those activities to continue smoothly while protecting the health information that is shared.

The health care definition below also appears to include labs as providing health care even if the lab is not a covered entity.

*160.103 Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:*

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and*
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.*

## **HHS Guidance Document 2002**

### **Other Situations in Which a Business Associate Contract Is NOT Required**

When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. 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.

-With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

-With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.

### **Q: Is a business associate contract required with organizations or persons where inadvertent contact with protected health information may result – such as in the case of janitorial services?**

**A:** A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, 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 protected health information, and any disclosure of protected health information 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. Such disclosures are incidental and permitted by the HIPAA Privacy Rule. See 45 CFR 164.502(a)(1).

If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), 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.

### **Q: Is a software vendor a business associate of a covered entity?**

**A:** The 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 protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity. For example, 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 protected health information.

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. See the definition of "workforce" at 45 CFR 160.103.

#### **Covered Entity liability for the actions of a Business Associate**

The Privacy Rule does not require a covered entity to actively monitor the actions of its business associates nor is the covered entity responsible or liable for the actions of its business associates. Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation. See § 164.504(e)(1).

#### **American Recovery & Reinvestment Act (ARRA) on Business Associates 2009**

##### **SEC. 13401. APPLICATION OF SECURITY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS.**

(a) Application of Security Provisions- Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) Application of Civil and Criminal Penalties- In the case of a business associate that violates any security provision specified in subsection (a), sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

(c) Annual Guidance- For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary of Health and Human Services shall, in consultation with industry stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date before the enactment of this Act.

#### **SEC. 13404. ARRA HITECH law 2009**

##### **APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES.**

(a) Application of Contract Requirements- In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity. (b) Application of Knowledge Elements Associated With Contracts- Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.

(c) Application of Civil and Criminal Penalties- In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42

U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act.

## **Changes from the HITECH Bill Guidance from a Law Firm**

### **Summary of HIPAA Changes Under the HITECH ACT**

#### **(1) Security Rule Provisions now apply to Business Associates**

Several provisions of the HIPAA Security Rule now apply to businesses associates of covered entities in the same manner that those provisions apply to covered entities. Business associates are organizations that provide services to ambulance service providers that have access to protected health information (“PHI”). Business associates include: compliance auditors, consultants, accounting services, and third party billing services. The new law would apply four sections of the Security Rule to business associates (45 C.F.R. §§164.308, 164.310, 164.312, and 164.316). So, business associates now have a duty under HIPAA to protect the confidentiality of all electronic protected health information (“ePHI”) that they utilize or disclose in performing functions for covered entities. Generally, business associates will now have to:

- Establish administrative safeguards to protect ePHI (45 CFR §164.308);
- Implement physical safeguards to limit physical access to ePHI (45 CFR §164.310);
- Implement technical safeguards for electronic information systems that control access to ePHI (45 CFR §164.312); and
- Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule and maintain proper documentation (45 CFR §164.316).

Business associates may already have these safeguards in place because they are required to do so under a business associate agreement. However, business associates should ensure that they have a formal compliance program consistent with the requirements of this new law.

#### **(2) Privacy Rule Contract Provisions now apply to Business Associates**

Business associates that are contracted with covered entities to perform services on their behalf are now directly covered under provisions of the Privacy Rule relating to contractual arrangements between covered entities and business associates.

Business associates who obtain or create PHI pursuant to a contract (or other written agreement), now have a legal duty to ensure that they are only using or disclosing PHI in accordance with 45 CFR §164.504(e). Section 164.504(e) lays out the necessary terms that must be in a contract between a covered entity and a business associate to ensure that information is only used for authorized purposes. Generally, the provision states that contracts between business associates and covered entities must establish the permitted and required uses and disclosures of PHI and provide that the business associate will not use or further disclose the information other than as permitted or required by the contract, or as required by law. The new law makes it clear that business associates cannot use or disclose PHI in violation of these requirements (which should be outlined in every agreement with a covered entity).

Secondly, the law states that business associates are now in violation of HIPAA if they know of a pattern of activity or practice of the covered entity that constitutes a violation of the covered entity’s obligation

under the contract (or other arrangement). Under the current law, a covered entity is charged with the duty to police the business associate's compliance with a contract between it and a business associate. Now, if business associates know that a covered entity is violating its duty under a contract, they too have a legal obligation under 45 CFR §164.504(e)(1)(ii) to take reasonable steps to try to stop the violation.

### **(3) New Requirements for Business Associate Agreements**

Any additional requirements of the bill that relate to security and privacy that are made applicable to covered entities should also be incorporated into the business associate agreements between the business associate and the covered entity.

### **(15) Business Associate Agreements Required for All Entities that Provide Transmission of PHI to Covered Entities and Business Associates**

Under the stimulus bill, any organization that provides data transmission of protected PHI to a covered entity or its business associate or any vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) with the covered entity or business associate. That contract must meet all HIPAA requirements. Covered entities are already required to do so and business associates are required to do so under this new law. The law also creates a legal duty for other organizations, such as health information exchange organizations, regional health information organizations and other vendors to enter into an agreement to protect PHI.

### **Red Flag Rules on Service Providers (Business Associates)**

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

*Section 1.90(b)(10) Service Provider.* The proposed and final regulations defined "service provider" as a person that provides a service directly to the financial institution or creditor. This definition was based upon the definition of "service provider" in the Information Security Standards.<sup>23</sup> (23) The Information Security Standards define "service provider" to mean any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through the provision of services directly to the financial institution. 12 CFR part 30, app. B (national banks).

## **HHS Guidance from the NPRM related to the regulations for implementation of HITECH Act Requirements July 2010**

### **Business Associate Agreements**

Sections 164.308(b) of the Security Rule and 164.502(e) of the Privacy Rule require a covered entity to enter into a contract or other written agreement or arrangement with its business associates. The purpose of these contracts or other arrangements, generally known as business associate agreements, is to provide some legal protection when protected health information is being handled by another person (a natural person or legal entity) on behalf of a covered entity.

The HIPAA Rules define “business associate” generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. We propose a number of modifications to the definition of “business associate.”

#### **a. Inclusion of Patient Safety Organizations**

We propose to add patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. PSQIA, at 42 U.S.C. 299b–22(i)(1), provides that Patient Safety Organizations (PSOs) must be treated as business associates when applying the Privacy Rule. PSQIA provides for the establishment of PSOs to receive reports of patient safety events or concerns from providers and provide analyses of events to reporting providers. A reporting provider may be a HIPAA covered entity and, thus, information reported to a PSO may include protected health information that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, *et seq.* While the HIPAA Rules as written would encompass a PSO as a business associate when the PSO was performing quality analyses and other activities on behalf of a covered health care provider, we propose this change to the definition of business associate to more clearly align the HIPAA and Patient Safety Rules.

**b. Inclusion of Health Information Organizations (HIO), E–Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records** Section 13408 of the HITECH Act, which became effective on February 18, 2010, provides that an organization, such as a Health Information Exchange Organization, E-prescribing Gateway, or Regional Health Information Organization, that provides data transmission of protected health information to a covered entity (or its business associate) and that requires access on a routine basis to such protected health information must be treated as a business associate for purposes of the Act and the HIPAA Privacy and Security Rules. Section 13408 also provides that a vendor that contracts with a covered entity to allow the covered entity to offer a personal health record to patients as part of the covered entity’s electronic health record shall be treated as a business associate.

Section 13408 requires that such organizations and vendors enter into a written business associate contract or other arrangement with the covered entity in accordance with the HIPAA Rules.

In accordance with the Act, we propose to modify the definition of “business associate” to explicitly designate these persons as business (3)(i) and (ii) of the definition, the term “business associate” would include: (1) 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 routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity. Section 13408 of the Act makes reference to Health Information Exchange Organizations; however, we instead include in the proposed definition the term “Health Information Organization” because it is our understanding that “Health Information Organization” is the more widely recognized and accepted term to describe an organization that oversees and governs the exchange of health related information among organizations.

Section 13408 also provides that the data transmission organizations that the Act requires to be treated as business associates are those that require access to protected health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates. This is consistent with our prior interpretation of the definition of “business associate,” through which we have indicated that entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates. See [http:// www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html](http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html).

In contrast, however, entities that manage the exchange of protected health information through a network, including providing patient locator services and performing various oversight and governance functions for

electronic health information exchange, have more than “random” access to protected health information and thus, would fall within the definition of “business associate.”

**c. Inclusion of Subcontractors** We propose to add language in paragraph (3)(iii) of the definition of “business associate” to provide that subcontractors of a covered entity—*i.e.*, those persons that perform functions for or provide services to a business associate, other than in the capacity as a member of the business associate’s workforce, are also business associates to the extent that they require access to protected health information. We also propose to include a definition of “subcontractor” in § 160.103 to make clear that a subcontractor is a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. Even though we use the term “subcontractor,” which implies there is a contract in place between the parties, we note that the definition would apply to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person. We request comment on the use of the term “subcontractor” and its proposed definition.

The proposed modifications are similar in structure and effect to the Privacy Rule’s initial extension of privacy protections from covered entities to business associates through contract requirements to protect downstream protected health information. The proposed provisions avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity. Allowing such a lapse in privacy and security protections may allow business associates to avoid liability imposed upon them by sections 13401 and 13404 of the Act, thus circumventing the congressional intent underlying these provisions. The proposed definition of “subcontractor” also is consistent with Congress’ overall concern that the privacy and security protections of the HIPAA Rules extend beyond covered entities to those entities that create or receive protected health information in order for the covered entity to perform its health care functions. For example, as discussed above, section 13408 makes explicit that certain types of entities providing services to covered entities—*e.g.*, vendors of personal health records—shall be considered business associates.

Therefore, consistent with Congress’ intent in sections 13401 and 13404 of the Act, as well as its overall concern that the HIPAA Rules extend beyond covered entities to those entities that create or receive protected health information, we propose that downstream entities that work at the direction of or on behalf of a business associate and handle protected health information would also be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary business associate, and likewise would incur liability for acts of noncompliance. We note, and further explain below, that this proposed modification **would not require the covered entity to have a contract with the subcontractor; rather, the obligation would remain on each business associate to obtain satisfactory assurances in the form of a written contract** or other arrangement that a subcontractor will appropriately safeguard protected health information. For example, under this proposal, if a business associate, such as a third party administrator, hires a company to handle document and media shredding to securely dispose of paper and electronic protected health information, then the shredding company would be directly required to comply with the applicable requirements of the HIPAA Security Rule (*e.g.*, with respect to proper disposal of electronic media) and the Privacy Rule (*e.g.*, with respect to limiting its uses and disclosures of the protected health information in accordance with its contract with the business associate).

**d. Exceptions to Business Associate** - We also propose to move the provisions at §§ 164.308(b)(2) and 164.502(e)(1)(ii) to the definition of business associate. These provisions provide that in certain circumstances, such as when a covered entity discloses protected health information to a health care provider concerning the treatment of an individual, a covered entity is not required to enter into a business associate contract or other arrangement with the recipient of the protected health information. While we do not change the meaning of these provisions, we believe these limitations on the scope of “business associate” are more appropriately placed in the definition as exceptions to the term to make clear that the Department does not consider the recipients of the protected health information in these circumstances to be business associates.

The movement of these exceptions and refinement of the definition of “business associate” also would help clarify that a person is a business associate if it 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 contract with the business associate.

#### **e. Technical Changes to the Definition**

For clarity and consistency, we also propose to change the term “individually identifiable health information” in the current definition of “business associate” to “protected health information,” since a business associate has no obligations under the HIPAA Rules with respect to individually identifiable health information that is not protected health information.

#### **5. Definition of “Protected Health Information”**

We propose to modify the definition of “protected health information” at § 160.103 to provide that the Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years. This proposed modification is explained more fully below in Section VI.E. of the preamble where we discuss the proposed changes to the Privacy Rule related to the protected health information of decedents.

**6. Definition of “Respondent”** The definition of the term “Respondent,” which is currently in § 160.302, would be moved to § 160.103. **A reference to “business associate” would be added following the reference to “covered entity” in recognition of the potential liability imposed on business associates** for violations of certain provisions of the Privacy and Security Rules by sections 13401 and 13404 of the Act.

**8. Definition of “Workforce”** - The HITECH Act is directly applicable to business associates and has extended liability for compliance with certain provisions of the Privacy and Security Rules to business associates. Because some provisions of the Act and the Privacy and Security Rules place obligations on the business associate with respect to workforce members, we propose to revise the definition of “workforce member” in § 160.103 to make clear that such term includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a business associate, is under the direct control of the business associate.