

BUSINESS ASSOCIATES

[45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)]

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity’s duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate’s independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Provision. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

What Is a “Business Associate?” A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

- A member of the covered entity’s workforce is not a business associate.
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

- *Business associate functions and activities include:* claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
- *Business associate services are:* legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

See the definition of “business associate” at 45 CFR 160.103.

Examples of Business Associates.

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

Business Associate Contracts. A covered entity’s contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the business associate;
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and

- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Sample business associate contract language is available on the HHS OCR Privacy of Health Information website at <http://www.hhs.gov/ocr/hipaa/contractprov.html>.

Transition Provisions for Existing Contracts. Covered entities (other than small health plans) that have an existing contract (or other written agreement) with a business associate prior to October 15, 2002, are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with the Privacy Rule, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under the Rule.

See 45 CFR 164.532(d) and (e).

Exceptions to the Business Associate Standard. The Privacy Rule includes the following exceptions to the business associate standard. See 45 CFR 164.502(e). In these situations, a covered entity is not required to have a business associate contract or other written agreement in place before protected health information may be disclosed to the person or entity.

- Disclosures by a covered entity to a health care provider for treatment of the individual.

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 protected health information for the treatment of an individual.
 - ▶ A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.
- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.
 - The collection and sharing of protected health information by a health plan that is a public benefits program, such as Medicare, and an agency other than the agency administering the health plan, such as the Social Security Administration, that collects protected health information to determine eligibility or enrollment, or determines eligibility or enrollment, for the government program, where the joint activities are authorized by law.

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.
- Among covered entities who participate in an organized health care arrangement

(OHCA) to make disclosures that relate to the joint health care activities of the OHCA.

- Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.
- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.
- To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of “business associate” at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.
- When a financial institution 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. When it conducts these activities, 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.

BUSINESS ASSOCIATES

Frequently Asked Questions

Q: Has the Secretary exceeded the HIPAA statutory authority by requiring “satisfactory assurances” for disclosures to business associates?

A: No. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity’s having a written contract with that business associate.

Q: Has the Secretary exceeded the HIPAA statutory authority by requiring “business associates” to comply with the Privacy Rule, even if that requirement is through a contract?

A: The HIPAA Privacy Rule does not “pass through” its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information.

Q: What are a covered entity’s obligations under the HIPAA Privacy Rule with respect to protected health information held by a business associate during the contract transition period?

A: During the contract transition period, covered entities must observe the following responsibilities with respect to protected health information held by their business associates:

- Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.
- Fulfill an individual's rights to access and amend his or her protected health information contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.
- Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of protected health information by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose protected health information to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.

Q: I have an existing contract with a business associate that will renew automatically before April 14, 2003. Does this automatic renewal mean I have to modify the contract by April 14, 2003, to make it compliant with the HIPAA Privacy Rule's business associate contract provisions or can I still take advantage of the transition period?

A: Evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002, are eligible for the transition period. The automatic renewal of a contract itself does not terminate qualification for the transition period, or the transition period itself. Renewal or modification for the purposes of the transition provisions requires action by the parties involved. For example, an automatic inflation adjustment to the price of a contract does not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before April 14, 2003.

Q: Is a covered entity liable for, or required to monitor, the actions of its business associates?

A: No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

Q: Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule?

A: No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at 45 CFR 164.504(e).

Q: Are accreditation organizations business associates of the covered entities they accredit?

A: Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of “business associate” at 45 CFR 160.103. Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See 45 CFR 164.514(e). If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

Q: Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

A: No. Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103. However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by Rule, that is, with an individual's authorization pursuant to 45 CFR 164.508, without an individual's authorization as permitted by 45 CFR 164.512(i), or as a limited data set provided that a data use agreement is in place as permitted by 45 CFR 164.514(e).

Q: When is a health care provider a business associate of another health care provider?

A: 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 protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. 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 patient health information.

Q: May a covered entity share protected health information directly with another covered entity's business associate?

A: Yes. If the HIPAA Privacy Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

Q: Are covered entities that engage in joint activities under an organized health care arrangement (OHCA) required to have business associate contracts with each other?

A: No. Covered entities that participate in an OHCA are permitted to share protected health information for the joint health care activities of the OHCA without entering into business associate contracts with each other. Of course, each such entity is independently required to observe its obligations under the HIPAA Privacy Rule with respect to protected health information.

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 physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

A: No, plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate". Under the HIPAA Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See the definition of "business associate" at 45 CFR 160.103.

Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See 45 CFR 164.502(a)(1).

Q: Are the following entities considered “business associates” under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

A: No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

Q: Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?

A: The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard protected health information, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting, as provided for by 45 CFR 164.524, 164.526, and 164.528. With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must make such protected health information available if and when needed by the covered entity to provide an individual with access to the information. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the designated record set, or part thereof.

Under 45 CFR 164.526, a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must amend protected health information in such records (or copies) when requested by the covered entity. The covered entity itself is responsible for addressing requests from individuals for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

Under 45 CFR 164.528, the Privacy Rule requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.

Q: Would a business associate contract in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's business associate contract requirements?

A: Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including business associate contracts, to qualify as written documents for purposes of meeting the Rule's requirements. However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

Q: Do physicians with hospital privileges have to enter into business associate contracts with the hospital?

A: No. The hospital and such physicians participate in what the HIPAA Privacy Rule defines as an organized health care arrangement (OHCA). Thus, they may use and disclose protected health information for the joint health care activities of the OHCA without entering into a business associate agreement.

Q: Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to

create de-identified data?

A: Yes. See 45 CFR 164.514(e)(3)(ii). For example, if a researcher needs county data, but the covered entity's data contains only the postal address of the individual, a business associate may be used to convert the covered entity's geographical information into that needed by the researcher. In addition, the covered entity may hire the intended recipient of the limited data set as the business associate for this purpose in accordance with the business associate requirements. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the recipient's request. However, the data recipient, as a business associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data use agreement and business associate contract?

A: Yes. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the covered entity is providing the recipient with protected health information that includes direct identifiers, a business associate agreement would be required in addition to the data use agreement to protect the information. For example, the agreement must require that the recipient agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

A: No. Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement. For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.

Q: Are business associates required to restrict their uses and disclosures to the

minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

A: A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

Q: Is a physician or other provider considered to be a business associate of a health plan or other payer?

A: Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "business associate" at 45 CFR 160.103.

Q: Is a health insurance issuer or HMO who provides health insurance or health coverage to a group health plan a business associate of the group health plan?

A: A health insurance issuer or HMO does not become a business associate simply by providing health insurance or health coverage to a group health plan. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an organized health care arrangement (OHCA), with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA. However, where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the joint activity of providing insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services.

Q: Is a reinsurer a business associate of a health plan?

A: Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.

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.