**Overview.**

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 (i.e., business associates).

**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. For the avoidance of doubt, if it is indicated anywhere that a business association agreement is not required, that necessarily means that a business associate relationship does not exist.

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.
* The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates.
* 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.

**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 (i.e., the determination of a business association is in the negative).

* Disclosures by a covered entity to a health care provider for treatment of the individual. 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). 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.
* 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.
* 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.
  + 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 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.
  + 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.
* 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.
  + 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.
* 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 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.
  + An Organized Health Care Arrangement (OHCA) is a health care system that involves multiple covered entities working together under the Health Insurance Portability and Accountability Act (HIPAA)
* Do physicians with hospital privileges have to enter into business associate contracts with the hospital?
* 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.
* 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.
  + Generally, a reinsurer is not a business associate of a health plan. 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.
* 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.
  + 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.
  + 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, so no business associate agreement is necessary.
  + However, there is an exception to this. 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?
    - 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.
* 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.
* 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.

**Unique situations**

* **When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative?**
  + Answer:In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual’s written authorization, to disclose protected health information to a medical device company representative (medical device company) for the covered provider’s own treatment, payment, or health care operation purposes ([45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c)(1)), or for the treatment or payment purposes of a medical device company that is also a health care provider (45 CFR 164.506(c)(2), (3)). Additionally, the public health provisions of the Privacy Rule permit a covered provider to make disclosures, without an authorization, to a medical device company or other person that is subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which the person has responsibility. See [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(b)(1)(iii) and the frequently asked questions on public health disclosures for more information.  
      
    In certain situations, a covered health care provider may disclose protected health information to a medical device company without an individual’s written authorization only if the medical device company is a health care provider as defined by the Rule. A medical device company meets the Privacy Rule’s definition of “health care provider” if it furnishes, bills, or is paid for “health care” in the normal course of business. “Health care” under the Rule means care, services or supplies related to the health of an individual. Thus, a device manufacturer is a health care provider under the Privacy Rule if it needs protected health information to counsel a surgeon on or determine the appropriate size or type of prosthesis for the surgeon to use during a patient’s surgery, or otherwise assists the doctor in adjusting a device for a particular patient. Similarly, when a device company needs protected health information to provide support and guidance to a patient, or to a doctor with respect to a particular patient, regarding the proper use or insertion of the device, it is providing “health care” and, therefore, is a health care provider when engaged in these services. See 65 FR 82569. By contrast, a medical device company is not providing “health care” if it simply sells its appropriately labeled products to another entity for that entity to use or dispense to individuals.  
      
    The following are some examples of circumstances in which a covered provider may share protected health information with a medical device company, without the individual’s authorization:
* A covered provider may disclose protected health information needed for an orthopaedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient’s surgery. (This would be a treatment disclosure to the device company as a health care provider. Exchanges of protected health information between health care providers for treatment of the individual are not subject to the minimum necessary standards. [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b).)
* The device manufacturer or its representative may be present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration or adjustment of a medical device for that particular patient. (This would be treatment by the device company as a health care provider. As noted in the prior example, treatment disclosures between health care providers are not subject to the minimum necessary standards.)
* A covered provider may allow a representative of a medical device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient’s treatment. (This would also be a treatment disclosure and minimum necessary would not apply.)
* A covered provider may share protected health information with a medical device company as necessary for the device company to receive payment for the health care it provides. (This would be a disclosure for payment of a health care provider and subject to minimum necessary standards.)
* A covered provider may disclose protected health information to a medical device manufacturer that is subject to FDA jurisdiction to report an adverse event, to track an FDA-regulated product, or other purposes related to the quality, safety, or effectiveness of the FDA-regulated product. (This would be a public health disclosure and subject to minimum necessary standards.)

A business associate agreement would not usually be required for the disclosures noted above. For example, a business associate agreement would not be needed for disclosures between health care providers for the treatment of the individual ([45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(e)(1)(ii)(A)). Likewise, a medical device company would not be a business associate of a covered provider with respect to public health disclosures to a device company that is subject to FDA jurisdiction or disclosures to a device company as a health care provider for that company’s payment purposes, as in neither case is the device company performing a function or activity on behalf of, nor providing a specified service to, the covered provider. See 45 CFR 160.103. In other circumstances, however, a business associate agreement may be required even if the disclosure were permitted without an authorization. For example, a business associate agreement would be required if a covered entity asked the medical device company to provide an estimate of the cost savings it might expect from the use of a particular medical device; and to do so, the device company needed access to the covered entity’s protected health information. In this case, the medical device company is performing a health care operations function (business planning and development) on behalf of the covered provider, which requires a business associate agreement even though the disclosure is permitted without an authorization.

* **When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?**
  + Answer: Under the Privacy Rule, a covered entity such as a doctor can contact a patient using a Telecommunications Relay Service (TRS), without the need for a business associate contract with the TRS. The sharing of protected health information between a covered health care provider and a patient through the TRS is permitted by the Privacy Rule under 45 C.F.R. 164.510(b), and a business associate contract is not required in these circumstances.  
      
    By way of background, the TRS enables telephone communication for people with hearing or speech impairments by using a communications assistant (CA) who transliterates conversations. The TRS CA relays information, which may include protected health information, between a text telephone (also known as “TTY”) user and another person communicating via voice. The CA must communicate what is said by the parties without alteration. The Federal Communications Commission (FCC), pursuant to the Americans with Disabilities Act (ADA), certifies all State TRS programs, which in turn contract with one or more TRS providers. All TRS providers must comply with standards for operators established by the FCC pursuant to Title IV of the ADA, including protecting the privacy of all relayed communications. The TRS is a public service that is available without cost to all persons and businesses, none of whom need to employ, contract with or otherwise establish business relationships with the TRS. Thus, when performing these services, the TRS is not acting for or on behalf of the covered entity and is not the covered entity’s business associate.  
      
    As permitted by [45 C.F.R. 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b), protected health information can be shared during a telephone communication using the TRS because the individual will have an opportunity to agree or object to disclosures of protected health information to the CA. The following typical scenarios describe how this opportunity can be provided in the course of, or prior to, using the TRS:
    - Where the individual initiates the call through the TRS, it is reasonable for a covered health care provider to infer from these circumstances that the individual has identified the CA as involved in the individual’s care, and that the individual does not object to the disclosure. See [45 C.F.R. 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b)(2)(iii).
    - Where the need for use of the TRS becomes apparent prior to a call being placed, such as when, during an office visit, the individual gives the health care provider his or her TTY number, the opportunity to agree or object to the TRS can be provided at that time. See 45 C.F.R. 164.510(b)(2).
    - Even where the covered health care provider initiates a call using the TRS without the individual’s prior agreement, the individual will have an opportunity to agree or object at the outset of the call. Typically, the CA will begin the call by identifying the service to the party called, and if that party is unfamiliar with the TRS, the CA will briefly explain how the service operates. This initial contact by the CA provides the individual with the opportunity to agree to the disclosure by proceeding with the call using the TRS, or to object by terminating the call. See 45 C.F.R. 164.510(b)(2)(i)-(ii).
* **In providing legal services to a covered entity, must a lawyer who is a business associate require that those persons to whom it discloses protected health information agree to abide by the privacy restrictions and conditions that apply to the lawyer**?
  + Answer:It depends on who the recipient is. The business associate agreement between the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) and the lawyer-business associate must provide that the lawyer will ensure that any agents, including subcontractors, to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate with respect to the information. See [45 CFR 164.504(e)(2)(ii)(D)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml).

Thus, if a lawyer-business associate enlists the services of a person or entity in furtherance of the lawyer’s legal services to a covered entity, and the lawyer must provide protected health information to the person or entity for such purpose, the lawyer’s business associate contract with the covered entity requires that the lawyer ensure that these persons agree to the same restrictions and conditions with respect to the protected health information they receive that apply to the lawyer as a business associate.

For example, pursuant to its business associate contract, a lawyer must ensure that other legal counsel, jury experts, document or file managers, investigators, litigation support personnel, or others hired by the lawyer to assist the lawyer in providing legal services to the covered entity, will also safeguard the privacy of the protected health information the lawyer receives to perform its duties. Conversely, a lawyer-business associate need not ensure that opposing counsel, fact witnesses, or other persons who do not perform functions or services that assist the lawyer in performing its services to the client, agree to the business associate restrictions and conditions, even though the lawyer may have to disclose protected health information to these third parties.

* **Must a covered health care provider obtain an individual’s authorization to use or disclose protected health information to an interpreter?**
  + Answer: No, when a covered health care provider uses an interpreter to communicate with an individual, the individual’s authorization is not required when the provider meets the conditions below. Covered entities may use and disclose protected health information for treatment, payment and health care operations without an individual’s authorization, [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c). A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

When using interpreter services, a covered entity may use and disclose protected health information regarding an individual without an individual’s authorization as a health care operation, in accordance with the Privacy Rule, in the following ways:

* When the interpreter is a member of the covered entity’s workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml);
* When a covered entity engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate, as defined at 45 CFR 160.103. A covered entity may disclose protected health information as necessary for the business associate to provide interpreter services on the covered entity’s behalf, subject to certain written satisfactory assurances set forth in [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e). For instance, many providers including those that are recipients of federal financial assistance and are required under Title VI of the Civil Rights Act of 1964 to take reasonable steps to provide meaningful access to persons with limited English proficiency -- will have contractual arrangements with private commercial companies, community-based organizations, or telephone interpreter service lines to provide such language services. If a covered entity has an ongoing contractual relationship with an interpreter service, that service arrangement should comply with the Privacy Rule business associate agreement requirements.

In addition, a covered health care provider may, without the individual’s authorization, use or disclose protected health information to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter. In these situations, that interpreter is not a business associate of the health care provider. As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the covered entity may obtain the individual’s agreement or reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure of protected health information to the interpreter. [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b)(2).  
  
For example, if a covered health care provider encounters a patient who speaks a language for which the provider has no employee, volunteer member of the workforce or contractor who can competently interpret, but then is able to identify a telephone interpreter service to communicate with the patient, the provider may contact the telephone interpreter service and identify the language used by the patient, so that the interpreter may explain to the patient that the interpreter is available to assist the patient in communicating with the provider. If the provider reasonably concludes that the patient has chosen to be assisted by the interpreter, and, by the patient’s willingness to continue the health care encounter using the interpreter, reasonably infers that the individual does not object to the disclosure, protected health information may be disclosed in accordance with [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b) without a business associate contract.  
  
Organizations that are subject to both HIPAA and Title VI must comply with the requirements of both laws, though not all HIPAA covered entities are recipients of federal financial assistance and thus, required to comply with Title VI; and not all recipients of federal financial assistance are also HIPAA covered entities, subject to the Privacy Rule. For information about the obligation of recipients of federal financial assistance to take reasonable steps to provide meaningful access to persons who are limited English proficient, see [Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons](https://www.hhs.gov/ocr/civilrights/resources/specialtopics/lep/factsheetguidanceforlep.html). This guidance includes information for recipients of federal financial assistance about important considerations for determining the competency of interpreters, such as their understanding of applicable confidentiality requirements, that should be taken into account when using interpreters arranged by the provider or when individuals elect to use friends, family or others as interpreters. HIPAA covered entities may also be required to comply with the Americans with Disabilities Act and/or Section 504 of the Rehabilitation Act of 1973, both of which have requirements for the provision of sign language and oral interpreters for people who are deaf or hard of hearing. See our [frequently asked question on the use of communications assistants as part of a Telecommunications Relay Service (TRS)](https://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/500.html).

* **If a CSP stores only encrypted ePHI and does not have a decryption key, is it a HIPAA business associate?**
  + Answer: Yes, because the CSP receives and maintains (e.g., to process and/or store) electronic protected health information (ePHI) for a covered entity or another business associate.  Lacking an encryption key for the encrypted data it receives and maintains does not exempt a CSP from business associate status and associated obligations under the HIPAA Rules.  An entity that maintains ePHI on behalf of a covered entity (or another business associate) is a business associate, even if the entity cannot actually view the ePHI.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2076/if-a-csp-stores-only-encrypted-ephi-and-does-not-have-a-decryption-key-is-it-a-hipaa-business-associate/index.html#_ftn1)  Thus, a CSP that maintains encrypted ePHI on behalf a covered entity (or another business associate) is a business associate, even if it does not hold a decryption key[[i]](https://www.hhs.gov/hipaa/for-professionals/faq/2076/if-a-csp-stores-only-encrypted-ephi-and-does-not-have-a-decryption-key-is-it-a-hipaa-business-associate/index.html#_edn1) and therefore cannot view the information.  For convenience purposes this guidance uses the term *no-view* *services* to describe the situation in which the CSP maintains encrypted ePHI on behalf of a covered entity (or another business associate) without having access to the decryption key.

While encryption protects ePHI by significantly reducing the risk of the information being viewed by unauthorized persons, such protections alone cannot adequately safeguard the confidentiality, integrity, and availability of ePHI as required by the Security Rule.  Encryption does not maintain the integrity and availability of the ePHI, such as ensuring that the information is not corrupted by malware, or ensuring through contingency planning that the data remains available to authorized persons even during emergency or disaster situations.  Further, encryption does not address other safeguards that are also important to maintaining confidentiality, such as administrative safeguards to analyze risks to the ePHI or physical safeguards for systems and servers that may house the ePHI.

As a business associate, a CSP providing no-view services is not exempt from any otherwise applicable requirements of the HIPAA Rules.  However, the requirements of the Rules are flexible and scalable to take into account the no-view nature of the services provided by the CSP.

* **Can a CSP be considered to be a “conduit” like the postal service, and, therefore, not a business associate that must comply with the HIPAA Rules?**
  + Answer:Generally, no. CSPs that provide cloud services to a covered entity or business associate that involve creating, receiving, or maintaining (e.g., to process and/or store) electronic protected health information (ePHI) meet the definition of a business associate, even if the CSP cannot view the ePHI because it is encrypted and the CSP does not have the decryption key.

As explained in previous guidance,[[i]](https://www.hhs.gov/hipaa/for-professionals/faq/2077/can-a-csp-be-considered-to-be-a-conduit-like-the-postal-service-and-therefore-not-a-business%20associate-that-must-comply-with-the-hipaa-rules/index.html#_edn1) the conduit exception is limited to transmission-only services for PHI (whether in electronic or paper form), including any temporary storage of PHI incident to such transmission. Any access to PHI by a conduit is only transient in nature. In contrast, a CSP that maintains ePHI for the purpose of storing it will qualify as a business associate, and not a conduit, even if the CSP does not actually view the information, because the entity has more persistent access to the ePHI.

Further, where a CSP provides transmission services for a covered entity or business associate customer, in addition to maintaining ePHI for purposes of processing and/or storing the information, the CSP is still a business associate with respect to such transmission of ePHI.  The conduit exception applies where the only services provided to a covered entity or business associate customer are for transmission of ePHI that do not involve any storage of the information other than on a temporary basis incident to the transmission service.

* **Do the HIPAA Rules allow health care providers to use mobile devices to access ePHI in a cloud?**
  + Answer: Yes. Health care providers, other covered entities, and business associates may use mobile devices to access electronic protected health information (ePHI) in a cloud as long as appropriate physical, administrative, and technical safeguards are in place to protect the confidentiality, integrity, and availability of the ePHI on the mobile device and in the cloud, and appropriate BAAs are in place with any third party service providers for the device and/or the cloud that will have access to the e-PHI.   The HIPAA Rules do not endorse or require specific types of technology, but rather establish the standards for how covered entities and business associates may use or disclose ePHI through certain technology while protecting the security of the ePHI by requiring analysis of the risks to the ePHI posed by such technology and implementation of reasonable and appropriate administrative, technical, and physical safeguards to address such risks.  OCR and ONC have issued guidance on the use of [mobile devices and tips](https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device) for securing ePHI on mobile devices.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2081/do-the-hipaa-rules-allow-health-care-providers-to-use-mobile-devices-to-access-ephi-in-a-cloud/index.html#_ftn1)
* **Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?**
  + Answer:Yes, provided the covered entity (or business associate) enters into a business associate agreement (BAA) with the CSP and otherwise complies with the applicable requirements of the HIPAA Rules. However, while the HIPAA Rules do not include requirements specific to protection of electronic protected health information (ePHI) processed or stored by a CSP or any other business associate outside of the United States, OCR notes that the risks to such ePHI may vary greatly depending on its geographic location. In particular, outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data. Covered entities (and business associates, including the CSP) should take these risks into account when conducting the risk analysis and risk management required by the Security Rule. See 45 CFR §§ 164.308(a)(1)(ii)(A) and (a)(1)(ii)(B). For example, if ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be considered, and entities must implement reasonable and appropriate technical safeguards to address such threats.
* **If a CSP receives and maintains only information that has been de-identified in accordance with the HIPAA Privacy Rule, is it a business associate?**
  + Answer: No. A CSP is not a business associate if it receives and maintains (e.g., to process and/or store) only information de-identified following the processes required by the Privacy Rule.  The Privacy Rule does not restrict the use or disclosure of de-identified information, nor does the Security Rule require that safeguards be applied to de-identified information, as the information is not considered protected health information. See the [OCR guidance on de-identification](https://www.hhs.gov/node/2960) for more information.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2085/if-a-csp-receives-and-maintains-only-information-that-has-been-de-identified-in-accordance-with-the-hipaa-privacy-rule-is-it-is-a-business-associate/index.html#_ftn1)