Purdue as the Business Associate

Derived from information provided by the Office for Civil Rights

As a HIPAA-covered employee, you should already be familiar with the HIPAA provisions that address safeguarding of protected health information by Purdue’s business associates. This article describes new issues that occur, when Purdue is the business associate.

Most covered 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. Business associate agreements are issued to all of Purdue’s business associates and these agreements are maintained by the HIPAA Privacy Compliance Office.

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. The term business associate is further defined on page 2 of this newsletter.

Under the HITECH Act, effective 2/17/2010, business associates must comply directly with HIPAA. These means that not only are business associates required to comply with the requirements of the business associate agreement, but they also need to comply with HIPAA’s Privacy and Security Rules and will be subject to fines as is any other covered component.

Implications for Purdue

Increasingly, areas at Purdue are becoming involved in projects where Purdue has access to or receives protected health information while performing a covered function on behalf of a covered entity. When Purdue enters into a business associate agreement, as is required in these cases, this triggers full coverage by the HIPAA laws. In order to identify the appropriate level of HIPAA involvement, either by the receipt of a business associate agreement or by the inclusion of HIPAA language within other agreements, contracts that include HIPAA language will be forwarded to the HIPAA Privacy Compliance Office where triggers for coverage or other issues can be identified. When coverage is necessary, the HIPAA Privacy Compliance Director will ensure that the proper procedures have been implemented and the employees provided HIPAA training. Also, ITaP Networks and Security will be notified when Security Rule compliance review is necessary.

Security Tip Trading Post

Security tips provided in the June SecurePurdue News

Tip #1: Many people use the gmail.com chat function to instant message with friends. Did you know Gmail automatically saves and archives these conversations for you? You have to manually turn off this function if you don’t want your instant message conversations saved. To do this, access your account settings through Gmail, click on chat settings, and select the button that says “never save chat history.”

Tip #2: Be careful what items you post on social networking sites. Items that you post, even if later you wish to remove them, may be difficult to remove or could remain available due to the high probability that the site or its contents have been saved or archived to an Internet Archive or have been shared or downloaded by someone.

Tip #3: Open Internet connections can expose your private and confidential information. Shut your computer down when you are not working on it.

Tip #4: If a scammer takes advantage of you through an online auction or through online shopping, you need to report it to the Federal Trade Commission, at http://ftc.gov

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa or contact: Joan Vaughan, Director, HIPAA Privacy Compliance telephone: (765) 496-1927 e-mail: jvaughan@purdue.edu
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 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.

**Exceptions to the Business Associate Standard.**
The Privacy Rule includes the following exceptions to the business associate standard. 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.
* 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 When a BA 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.

To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver or as a limited data set. 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”, 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.

---

**FAQ’s of the Month**

**Question:**
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, or for the treatment or payment purposes of a medical device company that is also a health care provider. 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.

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. 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.

---

Purdue University is an equal access/equal opportunity university.