Purdue has been designated as a hybrid entity under the HIPAA Rule. Hybrid entities have special compliance challenges and this article explains the concept and considerations involved in compliance under this designation.

**Hybrid Entities**

Under the Privacy Rule, any entity that meets the definition of a covered entity, regardless of size or complexity, generally will be subject in its entirety to the Privacy Rule. However, the Privacy Rule provides a means by which many covered entities may avoid global application of the Rule, through the hybrid entity designation provisions. This designation will establish which parts of the entity must comply with the Privacy Rule.

Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions or performs activities that would make the component a business associate of the entity if it were legally separate.

For example, a university may be a single legal entity that includes an academic health center that conducts electronic transactions for which HHS has adopted standards (e.g. billing). Because the health center is part of the legal entity, the whole university, including the health center, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the health center as a health care component. The university also has the option of including in the designation other components that conduct covered functions or business associate-like functions. Most of the Privacy Rule’s requirements would then only apply to the health center portion of the university and any other designated components. The Privacy Rule would govern only the PHI created, received, or maintained by, or on behalf of, these components. PHI disclosures by the health center to the rest of the university are regulated by the Privacy Rule in the same way as disclosures to entities outside the university.

Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the hybrid entity’s health care component(s) and be subject to the Privacy Rule. However, research components that function as health care providers, but do not conduct these electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, if the university in the example above also has a research laboratory that functions as a health care provider but does not engage in specified electronic transactions, the university as a hybrid entity has the option to include or exclude the research laboratory from its health care component. If such a research laboratory is included in the hybrid entity’s health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity’s health care component, the employees or workforce members of the laboratory are effectively not subject to the Privacy Rule.

**Disclosures by Covered Components of a Hybrid Entity**

Healthcare or health plan covered components within a hybrid entity, like Purdue, may only disclose protected health information (PHI), without a written authorization, to other entities that provide payment or health care operations on its behalf, for treatment purposes or for other purposes allowable under HIPAA. Except for treatment purposes, entities providing payment or healthcare operations on behalf of the covered healthcare provider or health plan will either be designated as covered components (if inside the University) or will be business associates (if vendors outside of the University). Other non-covered University departments may not receive access to a component’s PHI unless an authorization has been obtained form the individual who is the subject of the information or under certain conditions for research purposes. Business support components may disclose PHI but only to the covered provider or health plan providing the data to them, to other business support components for payment or healthcare operations purposes, or to their business associates. As always, if you are not sure whether a disclosure is allowed, contact the HIPAA Privacy Officer at hipaa-privacy@purdue.edu or x61927.

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](http://www.purdue.edu/hipaa) or contact: Joan Vaughan, HIPAA Privacy Officer, x61927.
Medical Identity Theft Q&A

What is medical identity theft?
The thief takes health insurance identification and uses it to receive health care or obtain reimbursements from insurers for false claims. Stolen credentials are most often used to obtain healthcare services, prescriptions or medical equipment.

Why do I care?
Medical Impact: People can die from this crime. Your medical history and the thief’s end up in the same file. Healthcare providers make diagnoses from the information in your file, resulting in inaccurate diagnoses and medical errors.

Financial Impact: For the individual, same as identity theft, unpaid bills, and negative credit reports, increase in premiums. For the hospital, loss of income, as they are unable to collect for the service the thief received.

Who does this?
Individuals who want or need expensive treatments steal or purchase stolen IDs. Or, vendors/providers will bill insurance using false claims.

How widespread a problem?
1.84 million adults or their family members became victims in 2012, significantly more than the 1.42 million in 2010 according to the Ponemon Institute.

Cost?
In addition to the potential medical risk, the monetary cost is ~$22,346 per victim.

Resolution?
Only 10% of the respondents to the Ponemon Institute survey on medical identity theft were able to completely resolve the consequences of the theft.

What can we do as guardians of protected health information?
The HIPAA Security rule requires protections be put into place that will greatly limit medical identity theft. Conduct a security risk analysis periodically (yearly) per NIST guide lines for HIPAA compliance. In addition to the Security Rule, be aware of Red Flags that may alert you to medical ID Theft. If a client questions a charge on a bill for a service they didn’t receive, investigate. If an ID appears questionable, ask questions. Be alert and aware to prevent and identify Medical Identity Theft.

For further information on this topic, please review the documents below.

http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf

Medical Identity Theft Q&A

When is Identifiable Health Information Not PHI?
The Privacy Rule applies only to covered entities. Many organizations that use, collect, access, and disclose individually identifiable health information will not be covered entities, and thus, will not have to comply with the Privacy Rule. To determine whether your organization is a covered component at Purdue, the Office for Civil Rights provides a decision tool that can be found at: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouACoveredEntity.html. The most current list of covered components at Purdue is found at: http://www.purdue.edu/hipaa/primary_menu/guidelines/components/index.shtml. If you believe that your area meets the definition of coverage, please contact the HIPAA Privacy Officer to discuss so that an official designation can be made, if necessary.

What is PHI?
The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity, its business associates or a business associates subcontractors, in any form or media, whether electronic, paper, or oral and refers to this information as Protected Health Information (PHI).

PHI is information, including demographic data, that relates to:
- the individual’s past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual,
  - and that identifies or can be used to identify the individual.

If the information is tied to a covered healthcare provider or health plan, then it is PHI by definition, since it is indicative that the individual received health care services or benefits from the covered component, and therefore it must be protected in accordance with the HIPAA Rules and any business associate agreements.

What is Not PHI?
The Privacy Rule excludes from the definition of PHI:
- employment records that a covered entity maintains solely in its capacity as an employer,
  - Examples: employee leave information, return to work documentation, FMLA documents, accommodation records maintained by Purdue Human Resources department
- education records subject to, or defined in, the Family Educational Rights and Privacy Act (FERPA)
- Health information about individuals who have been deceased for more than 50 years.


Purdue University is an equal access/equal opportunity university