Purdue is designated as a hybrid entity under HIPAA which means that only areas that meet the criteria for coverage must comply with the HIPAA Laws. Especially challenging has been the determination as to when researchers are part of a HIPAA-covered component. The following Q&A addresses these questions.

**When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule?**

If a covered entity decides to be a hybrid entity, it must define and designate its health care component(s). **Research components of a hybrid entity that function as health care providers and engage in standard electronic transactions (e.g., electronic billing) 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 engage in standard electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity’s 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 not subject to the Privacy Rule.

**When is a researcher considered to be a covered health care provider under HIPAA?**

A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule.

For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule.

**Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf.**

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

The HIPAA Privacy Officer 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
telephone: (765) 496-1927
e-mail: jvaughan@purdue.edu
How to Protect Electronic Health Information from Unauthorized Individuals

Article provided by ITaP Security and Policy

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

(i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved. Just deleting a file or folder does not purge the file. It can be recovered with a disk maintenance or undelete utility. Software tools are available to enable you to securely delete files. Ask your IT support for assistance.

FAQ’s from OCR

Provided by the Office for Civil Rights

Question:
Can an individual revoke his or her Authorization?

Answer:
Yes. The Privacy Rule gives individuals the right to revoke, at any time, an Authorization they have given. The revocation must be in writing, and is not effective until the covered entity receives it. In addition, a written revocation is not effective with respect to actions a covered entity took in reliance on a valid Authorization, or where the Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

The Privacy Rule requires that the Authorization must clearly state the individual’s right to revoke; and the process for revocation must either be set forth clearly on the Authorization itself, or if the covered entity creates the Authorization, and its Notice of Privacy Practices contains a clear description of the revocation process, the Authorization can refer to the Notice of Privacy Practices. Authorization forms created by or submitted through a third party should not imply that revocation is effective when the third party receives it, since the revocation is not effective until a covered entity which had previously been authorized to make the disclosure receives it.

Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an Authorization form that was prepared by a third party?

Answer:
Yes. A covered entity is permitted to use or disclose protected health information pursuant to an Authorization that meets the Privacy Rule’s requirements at 45 CFR 164.508. The Privacy Rule requires that an Authorization contain certain core elements and statements, but does not specify who may draft an Authorization (i.e., it could be drafted by any entity) or dictate any particular format for an Authorization. Thus, a covered entity may disclose protected health information as specified in a valid Authorization that has been created by another covered entity or a third party, such as an insurance company or researcher.