Included in this newsletter is guidance on various HIPAA-related topics that impact your everyday work life. Hopefully, it will help answer some of your questions about how HIPAA relates to your work processes.

Uses and Disclosures for Treatment, Payment, and Health Care Operations

Derived from guidance provided by the Office for Civil Rights

The HIPAA Privacy Rule establishes a foundation of Federal protection for personal health information, carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care. Ready access to treatment and efficient payment for health care, both of which require use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers and health plans, are essential to support treatment and payment. To avoid interfering with an individual’s access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

How the Rule Works

What are Treatment, Payment, and Health Care Operations?

“Treatment” generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

“Payment” encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

“Health care operations” are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

A covered entity may, without the individual’s authorization: Use or disclose protected health information for its own treatment, payment, and health care operations activities. For example:

- A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual’s treatment.
- A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
- A health plan may use protected health information to provide customer service to its enrollees.

A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule). For example:

- A primary care provider may send a copy of an individual’s medical record to a specialist who needs the information to treat the individual.
- A hospital may send a patient’s health care instructions to a nursing home to which the patient is transferred.

A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information. For example:

- A physician may send an individual’s health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.
- A hospital emergency department may give a patient’s payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment

A covered entity may disclose protected health information to another covered entity for certain health care

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, HIPAA Privacy Officer
telephone: (765) 496-1927
e-mail: hipaa-privacy@purdue.edu
University Data Handling Guidelines

Article derived from the SecurePurdue Best Practices site

University administrative data is an important University resource and asset. The University's administrative data is classified into three categories: Public, Sensitive, or Restricted. Based upon how the data is classified, that data may have certain precautions which need to be taken when handled.

Purdue's policy on Data Classification and Governance (VII.B.6) provides a framework for the governance and classification of University data in order to ensure the privacy and security of that data.

Personally-identifiable health information that is protected by the HIPAA Laws, PHI, is categorized as “restricted” data. The data handling guidelines referenced below, define how restricted information should be safeguarded while stored and transmitted. Please access the url: provided, for the handling guidelines associated with the specified forms of data.

How information should be handled is based upon the category of data that is contained in the document or electronic file. Information should be handled according to the highest classification level of data contained in the media. For example, if a data includes both Public and Restricted information, then the document or file should be handled according to the Restricted classification.

Handling of Printed Information (paper, microfiche, microfilm) (http://www.purdue.edu/securepurdue/procedures/dataHandling/printInfo1.cfm)

Electronically Stored (Computer-based) Information (http://www.purdue.edu/securepurdue/procedures/dataHandling/electStored.cfm)

Electronically Transmitted Information (http://www.purdue.edu/securepurdue/procedures/dataHandling/electTrans.cfm)

Data Custodians are encouraged to always use the most secure means possible to electronically transmit Purdue data. It is expected that departments will move toward encrypted transmission options over time and encourage their vendors and exchange agencies to move in this same direction. If an encryption option is available, it must be used for transmission of PHI.

Data is to be managed by a Data Steward as a University resource and asset. The Data Steward is responsible for facilitating the interpretation and implementation of the data policies and guidelines among their Vice President’s delegates. A list of the Data Stewards for each area can be found at: http://www.purdue.edu/securepurdue/policies/dataStewards.cfm#Membership

The Data Custodian is responsible for implementing the policies and guidelines established by the Data Steward. These responsibilities include physical data storage, back-up and recovery, and the operation of security and data management systems.

If you have any questions about how the data handling guidelines apply to the use or transmission of the PHI in your area, please contact your Data Steward for assistance. Purdue Data Custodians are urged to contact the Data Stewards for guidance in cases that present handling questions or security concerns.

FAQ’s from OCR

Question: Where the HIPAA Privacy Rule applies, does it permit a health care provider to disclose protected health information (PHI) about a patient to law enforcement, family members, or others if the provider believes the patient presents a serious danger to self or others?

Answer: The HIPAA Privacy Rule permits a covered entity to disclose PHI, including psychotherapy notes, when the covered entity has a good faith belief that the disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and (2) is to a person(s) reasonably able to prevent or lessen the threat. This may include, depending on the circumstances, disclosure to law enforcement, family members, the target of the threat, or others who the covered entity has a good faith belief can mitigate the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 CFR § 164.512(j)(1)(i). For example, consistent with other law and ethical standards, a mental health provider whose teenage patient has made a credible threat to inflict serious and imminent bodily harm on one or more fellow students may alert law enforcement, a parent or other family member, school administrators or campus police, or others the provider believes may be able to prevent or lessen the chance of harm. In such cases, the covered entity is presumed to have acted in good faith where its belief is based upon the covered entity’s actual knowledge (i.e., based on the covered entity’s own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member or other person). See 45 CFR § 164.512(j)(4).

For threats or concerns that do not rise to the level of “serious and imminent,” other HIPAA Privacy Rule provisions may apply to permit the disclosure of PHI. For example, covered entities generally may disclose PHI about a minor child to the minor’s personal representative (e.g., a parent or legal guardian), consistent with state or other laws. See 45 CFR § 164.502(b).