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.

Joan Vaughan
Purdue University Student Health Center

From the Director

During each summer, Privacy and Security Assessments are conducted in each of the covered areas. It is a very busy time for the HIPAA Compliance Office as the covered components typically have more time to devote to these efforts and also to other projects which have HIPAA implications.

Pay special attention to the article regarding changes to the state Social Security Disclosure law on page 2. Our attorneys at Stuart & Branigin were able to secure an amendment to the law which eliminates the need to obtain a written consent prior to disclosing SSN when permitted by HIPAA and FERPA. Although, SSN should not be collected or disclosed unless absolutely required, this change eliminates the additional paperwork burden for staff when making the necessary disclosures.

What we can learn from this scenario is that NOT properly identifying patients and others at each step in the process, provides the opportunity for information and/or treatment errors. The HIPAA Privacy Compliance Office has provided Communication Guidelines that specify proper identification of individuals.

When an individual requests information related to their treatment or payment for healthcare:
Confirm the identity of the individual by asking for their:

- Full name (first, middle initial, last name),
- PUID (if a Purdue student or employee) and
- Date of birth.

If the individual is not a Purdue student or employee or does not have their PUID, also ask for local address.

Validating Identity Prior to Disclosing Protected Health Information

In order to meet patient privacy and security requirements under HIPAA, the identity of individuals requesting information needs to be verified prior to disclosing protected health information.

Consider the following sample scenario:

Two patients enter a clinic for treatment purposes, their identities are verified and they are checked-in. The chart for each patient is sent to the provider. Each patient has the same first name. The patients are both in the lobby waiting for an appointment. When it is time for the patient to be seen by the doctor, the patient’s first name is called. One of the patients walks into the examination room. The other patient was on their cell phone and does not hear their name being called. The patient is treated and the diagnosis and services are entered into the patient chart. A prescription is given based on the medical history of the patient and a patient label is placed on the prescription. A bill is generated and sent to the patient. The patient takes the prescription to the Pharmacy and the prescription is filled. The patient takes the prescription and has an allergic reaction to the medicine. In this scenario, the identity of the patient was never validated after the initial check-in process. All other staff assumed that the patient’s identity was validated at the beginning of the process.

In this scenario,

- incorrect information was entered into another patient’s chart,
- an error was made in prescribing a drug,
- a bill indicating treatment was sent to the wrong patient, and
- information regarding another patient’s treatment was disclosed to an other patient.

What we can learn from this scenario is that NOT properly identifying patients and others at each step in the process, provides the opportunity for information and/or treatment errors. The HIPAA Privacy Compliance Office has provided Communication Guidelines that specify proper identification of individuals.

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

(Continued on page 2)
Disclosures to Family, Friends and Others Who are Involved in Patient Care or Payment

Still unsure as to when you can disclose PHI to those who are accompanying patients to office visits or who call on the telephone requesting information?

The following guidance should help you to determine in which situations it is appropriate to disclose protected health information without a written HIPAA authorization.

**Staff may disclose protected health information (PHI):**

- to any person identified by the individual. The PHI must be directly related to that person’s involvement in the individual’s care or payment for that care.

- to notify a person who is responsible for the care of the individual of the individual’s location or general condition.

**You may disclose PHI under these conditions:**

If the individual is present or available prior to the disclosure, and

- you have asked the individual if it is okay to disclose the information,

- you have given the individual an opportunity to object, or you can reasonably infer from the circumstances, based on professional judgment, that the individual does not object.

If the individual is not present you may use your professional judgment in determining that it is in the best interest of the individual to:

- disclose only the PHI that is directly relevant to a person’s involvement in the individual’s care or payment for care,

- allow a person to pick up filled prescriptions, medical supplies, X-rays or other forms of PHI.

**State SSN Disclosure Law - Update**

Great news! Purdue’s University legal counsel has secured an amendment to the Social Security Number (SSN) Disclosure law. This amendment eliminates the need by Purdue staff to obtain a consent to disclose SSN in most cases. The amendment was passed during the 2007 session and is effective immediately.

**Who is impacted by the change?**

Indiana state educational institutions.

**When or to whom can I disclose SSN, if required, without obtaining a written consent?**

Following are the additional disclosures of SSN authorized to occur without a written consent provided for within the amendment. Please review the legislation in its entirety for all authorized disclosures.

- A state, local, or federal agency or a person with whom a state, local, or federal agency has a contract to perform the agency’s duties and responsibilities.

- A person that Purdue contracts with to provide goods or services to Purdue if:
  - the disclosure is necessary for the contractor to perform the contractor’s duties and responsibilities under the contract; and
  - the contract requires adequate safeguards, including any safeguards required by state or federal law, to prevent any use or disclosure of the SSN for any purpose other than described in the contract and to require the return or confirmed destruction of any SSN following termination of the contract.

- Persons to whom the state educational institution may legally disclose for the permissible purposes of:
  - FERPA
  - HIPAA

- The state educational institution’s legal counsel, but only to the extent that a state educational institution could disclose a SSN to an in-house counsel.

Consent for the authorized disclosure of any individual’s SSN may be given to Purdue by **electronic transmission** if the state educational institution is reasonably able to verify the authenticity of the consent. Purdue may rely on the written consent of an individual given to a third party if the consent expressly permits the disclosure of the individual’s SSN by Purdue.

As always, social security number should be used, stored and/or disclosed only when absolutely necessary.


**Validating Identity Prior to Disclosing Protected Health Information (continued from page 1)**

For health plan benefits administrators:

When individuals request information about health plan claims or benefits specific to a health plan member, first determine the relationship of the individual to the health plan member and then follow the rules in the HIPAA Communication Guidelines to make proper identification and determination about what information can be shared. If an employee has restricted use or disclosure of information by the health plan, the restriction will be documented in a restriction folder. This folder will be maintained and any restrictions communicated to staff by the HIPAA Privacy Liaison for the Health Plan.

Additional details are provided in the HIPAA Communications Guidelines.

Please review and become familiar with the guidance in this document. The document can be found at: [http://www.purdue.edu/hipaa/guidelines/communicationguidelines.shtml](http://www.purdue.edu/hipaa/guidelines/communicationguidelines.shtml)

Purdue University is an equal access/equal opportunity university.