Validating Identity Prior to Sharing Information

As stated in Purdue's policy regarding Compliance with HIPAA Privacy Regulations policy VI.2.1., “Purdue University endeavors to preserve the privacy and confidentiality of the protected health information and medical records maintained by its various schools and departments.”

In order to meet patient privacy requirements under HIPAA, the identity of individuals requesting information needs to be verified prior to disclosing protected health information. The following guidelines should be used to validate identity:

**For health care providers and business support components:**
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.

**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 discussions 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)

Purchasing New Software or Making Software or Process Changes?

If either the purchase of new computer software or changes to existing software are planned in your area, and that software stores or provides access to protected health information, please notify your HIPAA liaison immediately.

The HIPAA liaison should contact the ITaP Security and Privacy department to be sure that the software’s security features are compliant with HIPAA, GLBA and FERPA regulations.

The liaison should also notify Joan Vaughan whenever there are material process changes planned in your area.

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, Director, HIPAA Privacy Compliance telephone: (765) 496-1927 e-mail: jvaughan@purdue.edu
Security Reminder - Incident Response

Purdue’s IT Security and Privacy area issued a new Incident Response policy. The following guidance was provided to help staff understand the procedures to use in reporting incidents. You can view the entire policy at: http://www.purdue.edu/policies/pages/information_technology/v_1_4.html

What to do when you suspect a security incident!

Do the following when you suspect a computer resource has been used inappropriately:

If the incident is considered a crime:
- Call your local police department to report the crime.
- Do not delete offending email from your computer until you have contacted your local police and they instruct you to do so.
- To report abuse of Purdue’s information technology resources, please fill out and submit the online incident report form. http://www.purdue.edu/securePurdue/incidentReportForm.cfm

If you are reporting inappropriate or objectionable email, or SPAM email, please forward the email to abuse@purdue.edu, and include the full headers of the email with your report.

Note: Complete the information on the Secure Purdue Incident page only if you think your problem is a serious IT incident. An IT incident is loosely defined as follows:
- violates the law
- constitutes harassment
- violates regulatory requirements
- violates Purdue policy
- compromises University data, or that of any person
- involves the unexpected disruption of University services

Examples of IT Incidents include:
- Accessing your computer or your data without permission or authority
- Hacking a University system
- Using University IT resources to hack into any non-University computer system
- Using University IT resources to harass or threaten someone
- Violating federal regulations with University IT resources
- Using University IT resources to harass or threaten someone
- Using University IT resources to access someone else’s computer system
- Using University IT resources to hack into any non-University computer system
- Using University IT resources to access someone else’s computer system
- Using University IT resources to harass or threaten someone
- Violating federal regulations with University IT resources
- Using University IT resources to hack into any non-University computer system
- Using University IT resources to access someone else’s computer system

University police telephone numbers for Purdue University campuses are listed below:
- West Lafayette campus, 765-494-8221
- Calumet campus, 219-989-2220
- North Central campus, 219-785-5220
- IU-PU Ft. Wayne campus, 260-481-6827

For more information please visit the Security Incident FAQs. http://www.purdue.edu/securepurdue/help/view.

FAQ of the Month

Answer:

No, when a covered health care provider uses an interpreter to communicate with an individual, the individual’s authorization is not required when the provider meets the conditions below. Covered entities may use and disclose protected health information for treatment, payment and health care operations without an individual’s authorization, 45 CFR 164.506(c). A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at 45 CFR 164.501.

When using interpreter services, a covered entity may use and disclose protected health information regarding an individual without an individual’s authorization as a health care operation, in accordance with the Privacy Rule, in the following ways:

- When the interpreter is a member of the covered entity’s workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at 45 CFR 160.103;
- When a covered entity engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate, as defined at 45 CFR 160.103. A covered entity may disclose protected health information as necessary for the business associate to provide interpreter services on the covered entity’s behalf, subject to certain written satisfactory assurances set forth in 45CFR 164.504(e).

At Purdue, if a covered component engages the assistance of a Purdue staff member to provide translation services and the staff member is not part of the workforce of the covered component, a HIPAA authorization would be required from the patient or the department in which the interpreter works would need to be designated as covered.

In addition, a covered health care provider may, without the individual’s authorization, use or disclose protected health information to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter. As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the covered entity may obtain the individual’s agreement or reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure of protected health information to the interpreter.