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**

New in this quarter are changes to the areas which are designated as covered by HIPAA at Purdue:

As of 9/4/2007, the following areas are now covered by HIPAA regulations:

- ITaP’s Unix and Windows Platform Administration and

Also, the designation of the Speech, Language and Hearing Sciences Department has changed. As of 9/5/07, the SLHS Audiology and Speech-Language Clinics are covered by the regulations as opposed to the entire SLHS department. This eliminates coverage for the majority of the researchers in SLHS.

In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient’s permission to share the information if doing so would interfere with the organization’s ability to respond to the emergency.

**IMMINENT DANGER:** Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider’s standards of ethical conduct.

**FACILITY DIRECTORY:** Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

---

### Sharing Health Care Information in a Severe Disaster

**Provided by the Office for Civil Rights**

Although I hope that you will never need the following guidelines, disasters do occur and covered components need to be prepared with knowledge regarding what information can be shared and in what circumstances during a disaster.

Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all of the following ways:

**TREATMENT:** Health care providers can share patient information as necessary to provide treatment.

**Treatment includes:**

- sharing information with other providers (including hospitals and clinics),
- referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
- coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

Providers can also share patient information to the extent necessary to seek payment for these health care services.

**NOTIFICATION:** Health care providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual’s care of the individual’s location, general condition, or death.

The health care provider should get verbal permission from individuals, when possible; but if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgement, doing so is in the patient’s best interest.

- Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.

**IMMINENT DANGER:** Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider’s standards of ethical conduct.

**FACILITY DIRECTORY:** Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

---

**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
Purdue University Password Requirements

One of the most important and simple-to-implement safeguards to protecting electronic health information is ensuring that system users select passwords that are difficult to guess for someone who may be attempting unauthorized access.

Following are Purdue’s password requirements. Although not all of Purdue’s systems support these requirements, as many as possible should be followed. **Please review and use the next time you create a new password.**

1. Passwords must contain at least 1 letter.
2. Passwords must contain at least 1 number or punctuation mark.
3. Passwords must be at least 8 characters long.
4. Passwords must contain more than 4 unique characters.
5. Passwords may not contain easily guessed words (e.g., Purdue, itap, boiler).
6. Passwords may not contain your name or parts of your name (e.g., Bill, Julie, Bob, or Susan).
7. New passwords must be different than the previous password (re-use of the same password will not be allowed for 180 days).
8. Passwords never should be stored on your computer or written down and stored in plain sight (e.g., taped to the bottom of your computer keyboard). If a password must be written down, it should be locked up and stored in a place that is difficult for others to access (i.e. your wallet).
9. Passwords may be used only by the authorized user. Do not share your password with anyone.
10. All users must change their password at least once every 30 days.

*** If you suspect your password has been compromised, it should be changed immediately.

BAD PASSWORDS

When picking passwords, AVOID the following:

- Your name, spouse’s name, or partner’s name.
- Your pet’s name or your child’s name.
- Names of close friends or coworkers.
- Names of your favorite fantasy characters.
- Your boss’s name.
- Anybody’s name.
- The name of the operating system you’re using.
- Information in the GECOS field of your passwd file entry
  - The hostname of your computer.
  - Your phone number or your license plate number.
  - Any part of your social security number.
  - Anybody’s birth date.
  - Other information easily obtained about you (e.g., address, alma mater).
  - Words such as wizard, guru, gandalf, boiler, Purdue, Pete and so on.
  - Any username on the computer in any form (as is, capitalized, doubled, etc.)

- A word in the English dictionary or in a foreign dictionary.
- Place names or any proper nouns.
- Passwords of all the same letter.
- Simple patterns of letters on the keyboard, like qwerty.
- Any of the above spelled backwards.
- Any of the above followed or preceded by a single digit.
- Password examples that have been published anywhere, including the examples in this document.


For more information on Purdue University’s Authentication and Authorization policy, as well as other policies related to information technology, please see [http://www.purdue.edu/policies/pages/information_technology/v_1_2.html](http://www.purdue.edu/policies/pages/information_technology/v_1_2.html).

FAQs of the Month

**Question:**
Can an Authorization be used together with other written instructions from the intended recipient of the information?

**Answer:**
A transmittal or cover letter can be used to narrow or provide specifics about a request for protected health information as described in an Authorization, but it cannot expand the scope of the Authorization. For example, if an individual has authorized the disclosure of “all medical records” to an insurance company, the insurance company could by cover letter narrow the request to the medical records for the last 12 months. The cover letter could also specify a particular employee or address for the “class of persons” designated in the Authorization to receive the information. By contrast, an insurance company could not by cover letter extend the expiration date of an Authorization, or expand the scope of information set forth in the Authorization.

**Question:**
May a covered entity accept documentation of an Institutional Review Board’s (IRB) waiver of authorization for purposes of reasonably relying on the request as the minimum necessary?

**Answer:**
Yes. The HIPAA Privacy Rule explicitly permits a covered entity to reasonably rely on a researcher’s documentation of an Institutional Review Board (IRB) or Privacy Board waiver of authorization pursuant to 45 CFR 164.512(i) that the information requested is the minimum necessary for the research purpose. See 45 CFR 164.514(d)(3)(iii).