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

or contact: Joan Vaughan, Director, HIPAA Privacy Compliance

telephone: (765) 496-1927

e-mail: jvaughan@purdue.edu

Research Disclosure Requirements

HIPAA protections extend to research, establishing the conditions under which covered entities might release personally identifiable health information for research purposes.

The basic rule is that research is not part of “treatment”, “payment” or “healthcare operations”, therefore the researcher must obtain a HIPAA authorization prior to receiving any protected health information for use in research.

Disclosures of protected health information by a covered component, for research purposes:

- require approval by the IRB,
- a signed informed consent, and
- authorization from the individuals or a waiver of authorization by the IRB.

Exceptions to this rule:

- IRB waiver,
- IRB modifications of authorization requirements,
- Reviews preparatory to research by staff of the covered component,
- Research involving a decedent’s information,
- Use of a limited data set.

The Privacy Rule requires covered entities to account for certain disclosures made after April 14, 2003, for a period of six (6) years, if requested to do so by an affected individual.

A covered component must account for disclosures made pursuant to an IRB waiver. The response must include:

- the name of the researcher,
- his/her contact information,
- the name of the study,
- a description of the purpose of the study and the type of protected health information sought, and the time frame of disclosures in response to the request.

The covered entity must also assist the individual in contacting those researchers to whom disclosure was likely made, if requested to do so.

Questions? Contact Joan Vaughan, x61927 or jvaughan@purdue.edu

Covered Component Changes:

The School of Nursing has opened two new clinics: the Family Health Clinic of Monon and the Trinity Nursing Center for Infant Health. Also, our Ft. Wayne campus is finalizing plans to open a clinic in mid-July or early August. This clinic will provide health, education and counseling services to the underserved population in Allen County in Northeast Indiana. The HIPAA Privacy Compliance Office has provided HIPAA training, policies and forms and has ensured that business associate agreements are in place where needed.

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

Research Disclosure Requirements

HIPAA protections extend to research, establishing the conditions under which covered entities might release personally identifiable health information for research purposes.

The basic rule is that research is not part of “treatment”, “payment” or “healthcare operations”, therefore the researcher must obtain a HIPAA authorization prior to receiving any protected health information for use in research.

Disclosures of protected health information by a covered component, for research purposes:

- require approval by the IRB,
- a signed informed consent, and
- authorization from the individuals or a waiver of authorization by the IRB.

Exceptions to this rule:

- IRB waiver,
- IRB modifications of authorization requirements,
- Reviews preparatory to research by staff of the covered component,
- Research involving a decedent’s information,
- Use of a limited data set.

The Privacy Rule requires covered entities to account for certain disclosures made after April 14, 2003, for a period of six (6) years, if requested to do so by an affected individual.

A covered component must account for disclosures made pursuant to an IRB waiver. The response must include:

- the name of the researcher,
- his/her contact information,
- the name of the study,
- a description of the purpose of the study and the type of protected health information sought, and the time frame of disclosures in response to the request.

The covered entity must also assist the individual in contacting those researchers to whom disclosure was likely made, if requested to do so.

Questions? Contact Joan Vaughan, x61927 or jvaughan@purdue.edu

Covered Component Changes:

The School of Nursing has opened two new clinics: the Family Health Clinic of Monon and the Trinity Nursing Center for Infant Health. Also, our Ft. Wayne campus is finalizing plans to open a clinic in mid-July or early August. This clinic will provide health, education and counseling services to the underserved population in Allen County in Northeast Indiana. The HIPAA Privacy Compliance Office has provided HIPAA training, policies and forms and has ensured that business associate agreements are in place where needed.

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.
Security Reminder - Computing Best Practices

As the security of protected health information is critically important to maintaining compliance with HIPAA, it is important that all staff receive information about computing safeguards.

ITaP has provided a list of Computing Best Practices to help secure the confidential information for which we are responsible. Following are some of the safeguards to keep in mind to secure your computer at work and at home:

- **Configure your operating system to automatically download and install the latest updates.**
- **Ensure all computers you use or control have up-to-date, supported, antivirus and anti-spyware software installed.** Configure the software to apply updates automatically. Configure your virus scan software and anti-spyware software to run a complete scan of your computer automatically at least once per week.
- **Turn on your Windows XP Internet Connection Firewall.**
- **Configure all workstations that access protected health information with a password-protected screensaver with no longer than a 15-minute timeout.**
- **Password changes must occur on every system or application accessing protected health information every 30 days.** Strong passwords should be used in all cases, where possible.
- **When off campus, access Purdue directories only through VPN.**

Before making any changes to the configuration of a Purdue computer, contact the workstation support group for your department.

State Law Reminder

In the March 2006 newsletter, information was introduced regarding two new state laws: one restricts the disclosure of social security number (SSN) outside of Purdue University and the other requires notification of individuals when an improper disclosure occurs.

“The penalties for violation of these laws are severe:”

An employee of a state agency who knowingly, intentionally or recklessly discloses an SSN in violation of this law or makes a false representation to a state agency to obtain an SSN, commits a **Class D felony.**

An employee of a state agency who negligibly discloses an SSN in violation of this law, commits a **Class A infraction.**

If you are not familiar with these laws or do not fully understand how they apply to your work, please refer to the HIPAA March 2006 newsletter at:

http://www.purdue.edu/hipaa/newsletters/newsletters.shtml and contact your supervisor or business office.

FAQ of the Month

**Question:**

May a health plan disclose protected health information to a person who calls the plan on the beneficiary’s behalf?

**Answer:**

Yes, subject to the conditions set forth in 45 CFR 164.510(b) of the HIPAA Privacy Rule. The Privacy Rule at 45 CFR 164.510(b) permits a health plan (or other covered entity) to disclose to a family member, relative, or close personal friend of the individual, the protected health information (PHI) directly relevant to that person’s involvement with the individual’s care or payment for care. A covered entity also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the covered entity has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment.

A covered entity only may disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

**For example:**

A health plan may disclose relevant PHI to a beneficiary’s daughter who has called to assist her hospitalized, elderly mother in resolving a claims or other payment issue.

A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.

A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional office’s assistance.

A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual’s concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person’s assistance.