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

What’s new in HIPAA privacy compliance at Purdue?

A new covered component was designated as of 2/1/2008, ITaP Customer Service Center. This group provides customer support for the OnePurdue system. This spring, a new adolescent treatment center is opening as part of the Trinity Nursing Center for Child Health. The clinic name has changed from Infant Health to reflect the new services offered. Also, the School of Nursing is investigating the purchase of a new medical records system for 4 of its clinics. The HIPAA Privacy Office will assist in the review of required safeguards to protect the data.

OCR Privacy Rule Enforcement Update

Information obtained from: http://www.hhs.gov/ocr/privacy/enforcement/01312008.html

The Office for Civil Rights (OCR) provides monthly statistics relating to its efforts to enforce the HIPAA Privacy Rule. The update has been provided here for your review of enforcement issues, as they may apply to your areas. Following is the January 2008 report.

Enforcement Results as of January 1, 2008

- HHS / OCR has investigated and resolved over 5,653 cases by requiring changes in privacy practices and other corrective actions by the covered entities. Corrective actions obtained by HHS from these entities have resulted in change that is systemic and that affects all the individuals they serve. HHS has successfully enforced the Privacy Rule by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

- In another 2,752 cases, our investigations found no violation had occurred.

- In the rest of our completed cases (17,983), HHS determined that the complaint did not present an eligible case for enforcement of the Privacy Rule. These include cases in which:
  - OCR lacks jurisdiction under HIPAA – such as a complaint alleging a violation prior to the compliance date or alleging a violation by an entity not covered by the Privacy Rule;
  - the complaint is untimely, or withdrawn or not pursued by the filer;
  - the activity described does not violate the Rule – such as when the covered entity has disclosed protected health information in circumstances in which the Rule permits such a disclosure.

In summary, since the compliance date in April 2003, HHS has received over 33,277 HIPAA Privacy complaints. We have resolved three quarters of complaints received (over 26,388): through investigation and enforcement (over 5,653); through investigation and finding no violation (2,752); and through closure of cases that were not eligible for enforcement (17,983).

From the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Uses or disclosures of more than the Minimum Necessary protected health information; and
- Lack of or invalid authorizations for uses and disclosures of protected health information.

Additional information about enforcement can be found at: http://www.hhs.gov/ocr/privacy/enforcement/

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
OCR Privacy Rule Enforcement Update
...Continued

The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

- Private Practices;
- General Hospitals;
- Outpatient Facilities;
- Health Plans (group health plans and health insurance issuers);
- and, Pharmacies.

Referrals
OCR refers to the Department of Justice (DOJ) for criminal investigation appropriate cases involving the knowing disclosure or obtaining of protected health information in violation of the Rule, and to the Centers for Medicare and Medicaid Services (CMS) for investigation appropriate cases that describe a potential violation of the HIPAA Security Rule. As of the date of this summary, OCR made over 419 such referrals to DOJ, and over 218 such referrals to CMS. In the referred cases that describe potential violations of both the HIPAA Privacy and Security Rules, OCR and CMS coordinate the investigations.

Outreach and Education
HHS also obtains privacy compliance through outreach and education efforts. OCR has reached hundreds of thousands of covered entities and consumers through educational conferences, a toll-free call line, and an interactive website. HHS has had over 5.5 million visits to its Privacy Web pages and over 4.3 million visits to the frequently asked questions on the Privacy Web pages. HHS has distributed announcements and educational information to over 18,000 subscribers to the Privacy listserv.

Security Concerns: File Sharing Tools
During the spring of 2008, ITaP will make Microsoft SharePoint available to University departments upon request. Among other things, the technology will allow staff to:

- easily share documents with anyone who meets a set of criteria,
- create collaborative websites called wikis,
- create online commentary or diaries called blogs, and
- manage document workflow support.

The document owner grants rights of access to the document as desired, to users who have a Purdue Career Account. The document can be made available to these users by the owner providing a url which points to the document.

The HIPAA Privacy Compliance Office has grave concern about the risk that staff will mistakenly grant access to documents containing protected health information (PHI), to those who are not authorized to view the information. Departments will need to evaluate how they may be able to use the new technology. Until the University community has had a chance to gain a better understanding or fully evaluate, please do NOT post any documents or content that contain PHI, using these tools.

FAQ of the Month
Provided by the Office for Civil Rights
http://www.hhs.gov/ocr/hipaa/

Question:

Does the HIPAA Privacy Rule’s public health provision permit covered health care providers to disclose protected health information concerning the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations to an individual’s employer?

Answer:

The public health provision permits covered health care providers to disclose an individual’s protected health information to the individual’s employer without authorization in very limited circumstances. First, the covered health care provider must provide the health care service to the individual at the request of the individual’s employer or as a member of the employer’s workforce. Second, the health care service provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. Third, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information. For example, OSHA requires employers to monitor employees’ exposures to certain substances and to take specific actions when an employee’s exposure level exceeds a specified limit. A covered entity which tests an individual for such an exposure level at the request of the individual’s employer may disclose that test result to the employer without authorization.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the protected health information the employer needs to meet such legal obligation may be discussed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there). When a health care service does not meet the above requirements, covered entities may not disclose an individual’s protected health information to the individual’s employer without an authorization, unless the disclosure is otherwise permitted without authorization by other provisions of the Rule. However, nothing in the Rule prohibits an employer from conditioning employment on an individual providing an authorization for the disclosure of such information.

Purdue University is an equal access/equal opportunity university.