From the Director

April 20, 2005 is the deadline for compliance with the HIPAA Security Rule. The purpose of the rule is to require administrative, physical and technical safeguards for the protection of electronic forms of protected health information. During the last several months, an assessment of the security environment in Purdue’s covered components has occurred. As a result, many policies and procedures have been developed in the individual departments and for the University, by ITaP Security and Privacy, to address the security of our data. In progress, is the completion of a risk assessment to determine what additional safeguards need to be put into place by April 20th and beyond.

Privacy and Security Safeguards

The HIPAA Privacy and Security Rules require that covered entities train staff regarding how to appropriately safeguard protected health information. Following are security guidelines for staff to keep in mind as they are working with confidential information:

DO NOT:

- remove any records, reports or copies of documents containing confidential or personal information from their storage location except as needed for the performance of job duties;
- use personal or confidential information to engage in illegal activities or to harass anyone;
- allow unauthorized use of information maintained, stored or processed in any electronic file, medical file, student file or computer system;
- access, use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so by giving them an employee access code, password or use of an employee’s equipment for any purposes not essential to the employee’s work.

DO:

- conduct confidential verbal conversations away from others who do not need to know;
- turn computer screens where PHI is viewed either away from the view of visitors or minimize applications while not in use;
- Never disclose your user id and password to anyone or allow anyone to access or alter information under the employee’s identity. Passwords should NEVER be posted near the work area or in a place that is easily accessible by other people.

(continued next page...Privacy and Security Safeguards...Continued)

Purchasing New Software or Making Software Changes?

If you are planning to either purchase new computer software or make changes to existing software in your area and that software stores or processes protected health information, please notify your HIPAA liaison immediately.

The HIPAA liaison should contact the ITaP Security and Policy department to be sure that the software’s security features are compliant with HIPAA, GLBA and FERPA regulations. The liaison will also notify Joan Vaughan for consideration of process changes.

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

Question:
May physicians offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

Answer:
Yes. Covered entities, such as physician’s offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician).

Disclosures to Family, Friends and Others Who are Involved in Patient Care or Payment

Given all of the restrictions HIPAA applies for sharing information, staff are sometimes confused about when they may disclose PHI to those who are accompanying patients to office visits or who call on the telephone requesting information. The following guidance should help staff determine in which situations it is appropriate to disclose protected health information.

Staff may disclose protected health information PHI):

\begin{itemize}
  \item 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.
  \item to notify a person who is responsible for the care of the individual of the individual’s location or general condition.
\end{itemize}

You may disclose PHI under these conditions:

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

\begin{itemize}
  \item you have asked the individual if it is okay to disclose the information,
  \item you have given the individual an opportunity to object, or
  \item you can reasonably infer from the circumstances, based on professional judgment, that the individual does not object.
\end{itemize}

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:

\begin{itemize}
  \item disclose only the PHI that is directly relevant to a person’s involvement in the individual’s care or payment for care,
  \item allow a person to pick up filled prescriptions, medical supplies, X-rays or other forms of PHI.
\end{itemize}