The HIPAA Privacy Rule establishes the conditions under which protected health information may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” A covered entity may always use or disclose for research purposes health information which has been de-identified without regard to the provisions below.

The Privacy Rule also defines the means by which individuals will be informed of uses and disclosures of their medical information for research purposes, and their rights to access information about them held by covered entities. Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research. Currently, most research involving human subjects operates under the Common Rule and/or the Food and Drug Administration’s (FDA) human subject protection regulations, which have some provisions that are similar to, but separate from, the Privacy Rule’s provisions for research. These human subject protection regulations, which apply to most Federally-funded and to some privately funded research, include protections to help ensure the privacy of subjects and the confidentiality of information. The Privacy Rule builds upon these existing Federal protections. More importantly, the Privacy Rule creates equal standards of privacy protection for research governed by the existing Federal human subject regulations and research that is not.

How the Rule Works

In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule.

Research Use/Disclosure Without Authorization. To use or disclose protected health information without authorization by the research participant, a covered entity must obtain one of the following:

- **Documented Institutional Review Board (IRB) or Privacy Board Approval.** Documentation that an alteration or waiver of research participants’ authorization for use/disclosure of information about them for research purposes has been approved by an IRB or a Privacy Board. This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants’ authorization were required. A covered entity may use or disclose protected health information for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board, provided it has obtained documentation of the alteration or waiver of authorization from the IRB or Privacy Board. Certain criteria need to be met for a waiver to be granted.

- **Preparatory to Research.** Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.

- **Research on Protected Health Information of Decedents.** Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought.

- **Limited Data Sets with a Data Use Agreement.** A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations. A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual. The data use agreement must:
  - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not

Continued on page 2
FAQ’s of the Month

How do HIPAA authorizations apply to an electronic health information exchange environment?

Answer:

The HIPAA Privacy Rule requires the individual’s written authorization for any use or disclosure of protected health information (PHI) not otherwise expressly permitted or required by the Privacy Rule. For example, authorizations are not generally required to disclose PHI for treatment, payment, or health care operations purposes because covered entities are permitted to use and disclose PHI for such purposes, with few exceptions. Thus, to the extent the primary purpose of any electronic health information exchange is to exchange clinical information among health care providers for treatment, HIPAA authorizations are unlikely to be a common method of effectuating individual choice for the exchange. However, if the purpose of a covered entity sharing PHI through a health information organization is for a purpose not otherwise permitted by the Privacy Rule, then a HIPAA authorization would be required. In such cases, the Privacy Rule would allow covered entities to disclose PHI pursuant to an electronic copy of a valid and signed authorization. Further, the Privacy Rule allows HIPAA authorizations to be obtained electronically from individuals, provided any electronic signature is valid under applicable law.

Phishing Scams-ITaP Offers Tips to Avoid Becoming a Victim

Provided by ITaP Security and Policy

In light of recent email phishing scams, ITaP reminds computer users never to provide personal information in response to an unsolicited email request. The University will never ask for your password or any other personal information through email.

Though some spam may look official, many unsolicited emails and instant messages containing URLs are actually attempts to trick recipients into divulging personal information or downloading a piece of malware on your machine.

“Phishing is the act of sending email falsely claiming to be from an established, legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft,” says Greg Hedrick, Purdue’s interim chief information security officer. “The email directs users to a website, where they are asked to update personal information — such as passwords and credit card, Social Security and bank account numbers — that the legitimate organization already has. The website, however, is bogus and set up only to steal users’ information. Links can also be a source of bad malware from an affected webpage used to steal passwords or documents stored on machines.”

The Federal Trade Commission website, http://www.ftc.gov, provides helpful information on a variety of technology security issues, including phishing. According to the site, users can help deter scammers by following these rules of thumb:

Don’t reply to email or pop-up messages that request personal or financial information, and never click on links in the message. Don’t cut-and-paste a link from the message into your Web browser, as scammers can make links look like they go one place but actually send users to a different site.

Scammers can send email that appears to be from a legitimate business asking recipients to call a phone number to update their account or access a “refund.” Because scammers use voice-over-Internet-protocol technology, the area code listed does not reflect the scammers’ actual location. When users need to reach an organization they do business with, they should call the number on their financial statements or on the back of their credit card.

Never email or instant message personal or financial information.

Review credit card and bank account statements as soon as you receive them for unauthorized charges.

Be cautious about opening attachments or downloading files from emails, regardless of who sent them. Files can contain viruses or other software that can weaken a computer’s security.

If there’s any doubt about the sender of an email or the destination of a URL, the message should be deleted immediately.

To report a suspicious email, contact abuse@purdue.edu.

For more information about computer security, please visit the SecurePurdue and Business Services Security websites.

Sources: Cherry Delaney, coordinator for security outreach and training, 765-496-1288, cdelaney@purdue.edu
Greg Hedrick, director of information security services and interim chief information security officer, 765-494-1875, hedrick@purdue.edu

Purdue University is an equal access/equal opportunity university