March 2010 Newsletter

Recruitment of Individuals into a Research Study Using the Preparatory Research Provision of the HIPAA Privacy Rule

Derived from Guidance Provided by the Office for Civil Rights

The preparatory research provision of the HIPAA Privacy Rule permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision does not permit the researcher to remove protected health information from the covered entity’s site. As such, a researcher who is an employee or a member of the covered entity’s workforce could use protected health information to contact prospective research subjects.

The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information.

Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization.

However, a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board. The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.

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
Targeted E-mail Scams Continue to Plague Purdue

From the Secure Purdue Newsletter-January 2010

The New Year has brought a resurgence in e-mail scams targeted specifically at Purdue University e-mail users. “These scams continue to plague campus,” said Greg Hedrick, Director of Security Services in ITaP Networks and Security. “Users should continue to question whether or not these e-mails are authentic before taking the action requested in the e-mail.”

The e-mails appear to come from various authoritative Purdue University administrative departments, such as the “Purdue Webmail Team,” “Purdue Management Team,” or “Purdue Support Team.” Often times these e-mails will look highly authentic, using Purdue logos, screenshots, or common Purdue terminology.

Some variations of these types of e-mails ask users to respond to the e-mail to confirm their e-mail address and to provide their computing login information and password. In most variations, the e-mails threaten that if the user does not respond or take some required action that their e-mail account will be somehow deactivated.

Not all of the e-mail scams are phishing attempts to gain user names and passwords. One of the latest scams targeted at Purdue attempts to download malicious software onto the end user’s computer.

This scam specifically targets Outlook Web Access (OWA) users. The e-mails direct users to navigate to a specific URL. Navigating to the web pages indicated in the e-mails and following directions on those web pages can potentially install malware on the user’s computer. Many anti-virus products, including McAfee, will detect and delete the malware. “Users who receive these types of e-mails should question whether they are from the university,” Hedrick said. “Users should immediately delete the e-mails and should not reply or take the action requested in the e-mail. In addition, IT units at Purdue will never ask users to divulge their passwords to university IT resources.”

**Users who have responded to e-mail scams such as the ones described here should immediately reset their Purdue Career Account password.** Users can go to the password reset page located at [www.purdue.edu/securepurdue](http://www.purdue.edu/securepurdue). (Click on the “Change Your Password” link on the bottom right hand side of the page.) Users who believe that they have been infected with malware should contact their local computer support groups for further assistance.

*For more information about computer security at Purdue, please access:* [http://www.purdue.edu/securePurdue/](http://www.purdue.edu/securePurdue/)

---

**FAQ’s of the Month**

Provided by the Office for Civil Rights

**Question:**

Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

**Answer:**

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

**Question:**

Does the HIPAA Privacy Rule limit what a doctor can do with a family medical history?

**Answer:**

Yes, if the doctor is a “covered entity” under the HIPAA Privacy Rule. A doctor, who conducts certain financial and administrative transactions electronically, such as electronically billing Medicare or other payers for health care services, is considered a covered health care provider. The HIPAA Privacy Rule limits how a covered health care provider may use or disclose protected health information. The HIPAA Privacy Rule allows a covered health care provider to use or disclose protected health information (other than psychotherapy notes), including family history information, for treatment, payment, and health care operation purposes without obtaining the individual’s written authorization or other agreement. The HIPAA Privacy Rule also generally allows covered entities to disclose protected health information without obtaining the individual’s written authorization or other agreement for certain purposes to benefit the public, for example, circumstances that involve public health research or health oversight activities.

When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual’s family medical history, this information becomes part of the individual’s medical record and is treated as “protected health information” about the individual. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record, including the right of access, amendment, and the ability to authorize disclosure to others.