PURDUE UNIVERSITY HIPAA Advisory

http://www.purdue.edu/hipaa

September 2011 Newsletter

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 processes.

Research-Recruitment of Subjects and Hybrid Entities

Derived from guidance provided by the Office for Civil Rights

HIPAA requirements provide additional challenges for researchers who are using protected health information in the process of conducting research. One of the issues to be addressed is use of patient information to recruit subjects into a research study. The preparatory research provision of the HIPAA Privacy Rule can be used for this purpose, but under the following conditions.

The preparatory research provision 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.

Hybrid Entities

Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the hybrid entity's health care component(s) and be subject to the Privacy Rule. However, research components that function as health care providers, but do not conduct these electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, if a university has a research laboratory that functions as a health care provider but does not engage in specified electronic transactions, the university as a hybrid entity has the option to include or exclude the research laboratory from its covered health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are effectively not subject to the Privacy Rule.

The hybrid entity is not permitted, however, to include in its health care component, a research component that does not function as a health care provider or does not conduct business associate-like functions. For example, a research component that conducts purely records research is not performing covered or business associate-like functions and, thus, cannot be included in the hybrid entity's health care component.

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

IT Security Incident Response

Provided by ITaP Networks and Security-Purdue University has had a formal process for responding to IT Incidents since 2005. It is important to handle IT incidents properly in order to repair and return compromised IT resources into production use as soon as possible, to learn if any confidential data was exposed, and to prevent similar attacks. Purdue University has a number of protocols and procedures to properly handle University IT incidents.

An IT Incident is any event involving University IT resources which:

- Violates local, state, or U.S. federal law;
- Violates a regulatory requirement that Purdue must honor;
- Violates a Purdue University policy;
- Is determined to be harmful to the security and privacy of University data, or IT Resources associated with, students, faculty, staff and/or the general public;
- Constitutes harassment under applicable law or University policy; or
- Involves the unexpected disruption of University services.

According to Greg Hedrick, Director of IT Security Services in ITaP Networks and Security, it is important to remember that any user of Purdue IT Resources must report an IT Incident, this includes departments and end users. "We have mechanisms in place so that any member of the Purdue community can easily report an IT Incident. There is a button to report a security incident on the SecurePurdue homepage. Individuals and department IT groups must report any suspicious computer activity. The sooner these incidents are reported, the faster we can go about protecting the University, its data, and our computer users," Hedrick said.

If you believe that your University owned computer device has been involved in an IT incident, you should use the "Report A Security Incident" link on the SecurePurdue (http://www.purdue.edu/securepurdue) website or send an email to abuse@purdue.edu to report the event.

IT Incidents must be reported immediately. In addition to reporting the incident:

- Do not use the computer system that is involved in the suspected incident.
- Do not shut down, turn off, or unplug (from electricity) the computer system that is involved in the suspected incident.
- Unplug the computer system that is involved in the suspected incident from Purdue's network if you are able to do so. Disconnect the network cable from the wall connector or the computer system, whichever is easiest to reach.

Finally, you should document any available relevant information about the event, including dates, times, persons/resources involved, and IP addresses. You can read more about what to do when you

FAQ of the Month

Provided by the Office for Civil Rights

FAQ

Question:

Under the HIPAA Privacy Rule, may a health care provider disclose protected health information about an individual to another provider, when such information is requested for the treatment of a family member of the individual?

Answer:

Yes. The HIPAA Privacy Rule permits a covered health care provider to use or disclose protected health information for treatment purposes. While in most cases, the treatment will be provided to the individual, the HIPAA Privacy Rule does allow the information to be used or disclosed for the treatment of others. Thus, the Rule does permit a doctor to disclose protected health information about a patient to another health care provider for the purpose of treating another patient (e.g., to assist the other health care provider with treating a family member of the doctor's patient). For example, an individual's doctor can provide information to the doctor of the individual's family member about the individual's adverse reactions to anesthetics prior to the family member undergoing surgery. These uses and disclosures are permitted without the individual's written authorization or other agreement with the exception of disclosures of psychotherapy notes, which requires the written authorization of the individual.

However, the HIPAA Privacy Rule permits but does not require a covered health care provider to disclose the requested protected health information. Thus, the doctor with the protected health information may decline to share the information even if the Rule would allow it. The HIPAA Privacy Rule may also impose other limitations on these disclosures. Under 45 CFR § 164.522, individuals have the right to request additional restrictions on the use or disclosure of protected health information for treatment, payment, or health care operations purposes. If the health care provider has agreed to the requested restriction, then the doctor is bound by that agreement and (except in emergency treatment situations) would not be permitted to share the information. However, the health care provider maintaining the records does not have to agree to the requested restriction. For example, an individual who has obtained a genetic test may request that the health care provider not use or disclose the test results. If the health care provider agrees to the restriction, the information could not be shared with providers treating other family members who are seeking to identify their own genetic health risks.

(Continued from IT Security Incident Response)

suspect a security incident at: http://www.purdue.edu/securepurdue/bestPractices/securityIncident.cfm

To learn more about computer security at Purdue, visit the SecurePurdue website at www.purdue.edu/securepurdue