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.

Appropriate Access to Protected Health Information

The HIPAA Privacy Rule specifies in what circumstances a covered component may use and disclose protected health information:

- for treatment,
- for payment of health care services,
- for healthcare operations,
- as authorized by the patient, and
- for other circumstances described in the Privacy Rule, (e.g. public health and as required by law).

All uses and disclosures should be limited to the minimum necessary information except:

- disclosures of PHI by a health care provider for treatment purposes,
- uses or disclosures made to the individual who is the subject of the information, and
- uses or disclosures pursuant to an authorization.

Purdue is a hybrid entity. Generally, only individuals reporting to departments that have been designated by the HIPAA Compliance Office as covered by HIPAA, may have access to protected health information and only if they are providing treatment, payment or healthcare operations functions on behalf of a Purdue covered healthcare provider or Purdue’s health plans. Providing HIPAA training to an individual does not authorize that person to receive access to protected health information. The person needs to be designated as covered workforce and then training is one of the requirements of coverage.

If a department is not included on the list of covered components and legitimately needs access to protected health information because they are providing a covered function, the following steps will be followed:

- Purdue’s HIPAA Privacy Officer should be contacted.
- A decision will be made regarding whether the use or disclosure is permitted by the Privacy Rule.
- The department will be designated as a Purdue covered component and a HIPAA liaison (departmental representative) will be named.
- The individuals who need access will be identified and trained.
- HIPAA privacy and security assessments will be completed periodically to review and document compliance.

Purdue’s current list of HIPAA covered components can be found at: http://www.purdue.edu/hipaa/primary_menu/guidelines/components/index.shtml

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, HIPAA Privacy Officer, jvaughan@purdue.edu or x61927
HIPAA requires organizations that handle protected health information to regularly review the administrative, physical and technical safeguards they have in place to protect the security of the information. By conducting these risk assessments, covered entities can uncover potential weaknesses in their security policies, processes and systems. Risk assessments also help us address vulnerabilities, potentially preventing health data breaches or other adverse security events.

One of the key initial steps in the risk assessment process is to identify the systems/hardware/software/data which store, process, or transmit electronic protected health information (ePHI). Covered Entities (CE) must also identify components of the organization which handle ePHI and the physical location of IT assets that contain ePHI. Lack of an accurate inventory of systems and an understanding of business use of ePHI will prevent Purdue from establishing an effective risk assessment process.

HIPAA Security Risk Assessments of Covered Entities begin with an inventory and a review of account access to those assets. This process is currently underway in Purdue’s covered components.

**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, CISO, Interim in the ITaP Security and Policy department, 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

**FAQ’s**

Does the HIPAA Privacy Rule protect genetic information?

**Answer:**

Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse.

**Additional Note:** Genetic information cannot be used for underwriting purposes except for Long Term Care policies.

(Continued from IT Security Incident Response)

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 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.