



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.

Reminders: General Safeguards

With the start of the school year and the many issues to think about and remember, it is a good time to remind workforce of some of the safeguards to use in protecting health information. Patients and health plan members DO notice when you take extra care in protecting their privacy and when you don't.

Safeguarding **SPOKEN** protected health information:

- ▶ Business Support Components should direct questions from individuals about bills or other PHI to the originating provider or health plan staff who can answer detailed questions,
- ▶ Confidential verbal conversations should be conducted away from others who do not need to know. Close doors or conduct discussions about PHI with individuals in a private office. Do not discuss PHI in public areas like waiting areas, hallways or elevators,
- ▶ Ask the individual's permission before speaking about their PHI in front of others accompanying them,
- ▶ Never use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so.



To safeguard protected health information **ON PAPER**, you must:

- ▶ Never leave papers unattended on printers, copiers, fax machines, etc.,
- ▶ Use a cover sheet when faxing PHI and check the fax number prior to using if unsure of the number,
- ▶ Documents containing PHI should not be left in open areas, mailboxes or on desks where they can easily be seen by passers by. Place these documents in folders or envelopes, turn them over or place a sheet of paper on top,
- ▶ Shred papers containing PHI when no longer needed or place in approved confidential destruction bins. "Don't throw it in the trash!",
- ▶ Ensure that appropriate physical safeguards are used to protect papers when not in use, like placing in locked file cabinets. Rooms and file cabinets where PHI is stored should be locked whenever staff are out of the office.

Safeguarding **ELECTRONIC PHI** means you should:

- ▶ Never send PHI through unencrypted e-mail. Use the Filelocker tool if electronic transmission is necessary, Computer screens where PHI is viewed should be turned away from the view of visitors and applications should be minimized while not in use,
- ▶ Do not ever disclose your user id or password to anyone (even computer support staff), or allow anyone to access or alter information under your identity,
- ▶ A password-protected screen saver with a timeout of no longer than 15 minutes is required on all workstations in HIPAA-covered areas. Always lock your workstation when leaving your work area,
- ▶ NEVER copy files containing PHI to a laptop or mobile device (e.g. Blackberry or FLASH drives),
- ▶ PHI should NEVER be stored on a local computer drive if a network drive is available for storage,
- ▶ As new tools become available to share electronic data with others, always discuss with the HIPAA Privacy Compliance Office prior to using these tools for documents containing PHI.

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



Tool Available for Encrypting and Transmitting Data



Given the fact that Purdue's email is not encrypted, it has been a challenge to securely transmit electronically-stored protected health information. Responding to this need, Purdue's ITaP has developed an open source program, **Filelocker**, for use by Purdue's faculty and staff to conveniently and securely share files with other people both on and off campus. In order to access the **Filelocker** application, the user must login in with their Purdue Career Account and password. Instructions on how to use this utility can be found at: http://www.purdue.edu/hipaa/primary_menu/procedures_forms/data/index.shtml

IT Policies Approved and Revised

Obtained from SecurePurdue News, June 2010

Purdue's Executive Policy Review Group (EPRG) approved one new and two revised IT policies at their February meeting.

The EPRG is a standing committee of Purdue University executives who provide institutional review, approval, or recommendation of approval of Purdue University System-Wide Policies. The president of the University appoints the committee members.

The **new policy** is the **Data Classification and Governance Policy (V.1.8)**. This policy was drafted and approved by the University Data Stewards, the Security Officers (SO) Working Group, and IT Networks and Security (ITNS). The policy formalizes the University's "public," "sensitive," and "restricted" data classifications.

The **revised policies** were drafted and approved by the SO Working Group and ITNS. The IT Executive Steering Committee approved them as well. They are:

Remote Access to IT Resources (V.1.6). This policy specifically allows remote access to University IT resources. Remote access is access to IT Resources from an electronic or other device not directly connected to the Purdue University wired or wireless networks, but not including accesses to such IT Resources where Remote Access is considered a primary function and normative use. For example, use of a Web browser to remotely access a Purdue University Web page is not covered by this policy. ITNS and the SO Group have issued a Remote Access Standard in support of this policy.

IT Resource Logging (V.1.7). This policy requires logging to be implemented on University IT Resources.



It recognizes that logging and log review is an important information security control.

Departments have flexibility in determining the detail contained in IT Resource logs for their area of responsibility. ITNS and the SO Group have issued a Basic Logging Standard in support of this policy.

All policies went into effect on March 1, 2010. They can be

...continued

FAQ's of the Month

Provided by the Office for Civil Rights



Question:

Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?

Answer:

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI.

The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

Question:

Does the Security Rule permit a covered entity to assign the same log-on ID or user ID to multiple employees?



Answer:

No. Under the Security Rule, covered entities, regardless of their size, are required, under § 164.312(a)(2)(i) to "assign a unique name and/or number for identifying and tracking user identity." A "user" is defined in § 164.304 as a "person or entity with authorized access." Accordingly, the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains electronic protected health information (e-PHI), so that system access and activity can be identified and tracked by user. This pertains to workforce members within small or large healthcare provider offices, health plans, group health plans, and healthcare clearing-houses.

IT policies approved and revised...continued

found at: http://www.purdue.edu/policies/pages/information_technology/info_tech.html

The new and revised policies were announced in the February 16, 2010 edition of Purdue Today.

The standards issued in support of the Remote Access and Logging policies are available at: <http://www.purdue.edu/securepurdue/bestPractices/ITStandards.cfm>.