PURDUE UNIVERSITY HIPAA Advisory
http://www.purdue.edu/hipaa

June 2009 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.

Incidental Uses and Disclosures

Article provided by the Department of Health and Human Services

Background

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally. For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

How the Rule Works

General Provision. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

Reasonable Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information – for instance:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets or records rooms; or
- By providing additional security, such as passwords, on computers maintaining personal information.

Protection of patient confidentiality is an important practice for many health care and health information manage ment professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

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

Educational Security Incidents - Review 2008

From the SecurePurdue News May 2009

The Educational Security Incidents (ESI) serves as a clearinghouse for compiling data on information security incidents that have occurred at higher educational institutions. ESI provides a single point of reference for educational faculty and staff researching the various security threats that colleges and universities face. In February 2009, ESI released its Year in Review-2008, which looks at the reported information security breaches that colleges and universities faced in 2008. The statistics are compiled using information security incidents at colleges and universities that were reported in news media.

In 2008, ESI reports that 173 different information security incidents occurred at 178 different colleges and universities; exposing a total of 4,880,052 records. The number of incidents reflects a 24.5% increase over 2007, and the average number of records exposed per incident is 28,208. ESI categorizes security incidents as follows:

Employee Fraud: Incidents involving fraudulent activity by employees (6% of 2008 incidents)

Theft: Incidents involving the theft of physical mediums such as drives, equipment, or printouts (23% of 2008 incidents)

Impersonation: Incidents involving one individual(s) masquerading as a different individual(s) or organization (2% of 2008 incidents)

Loss: Incidents involving the loss of physical mediums such as drives, equipment, or printouts (5% of 2008 incidents)

Penetration: Incidents involving the breach of computer software, a computer system or a computer network (20% of 2008 incidents)

Unauthorized Disclosure: Incidents involving the release of information to unknown and/or unauthorized individuals (44% of 2008 incidents)

ESI also catalogs the type of information exposed during a security incident. Those classifications are educational information, financial information, medical information, personally identifiable information, Social Security numbers, and usernames and passwords. The 2008 report shows that unauthorized disclosure of records continues to be the number one security incident at colleges and universities and personally identifiable information continues to be the most common information exposed.

Purdue University had no security incidents listed in the 2008 ESI report.

The statistics compiled by ESI illustrate that there are a number of types of confidential information held by colleges and universities that needs to be protected. Purdue University continues to take many steps to protect the personal information entrusted to it under the auspices of the SecurePurdue program. To read more about security awareness, visit www.purdue.edu/securepurdue.

March Article Correction

The article, titled "**How to Tell, What to Do, If Computer is Infected?**" should have included the following reference: http://www.msnbc.msn.com/id/29719417/ . Please refer to this site for the complete article.

FAQ of the Month

Derived from guidance provided by the Office for Civil Rights
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdfhipaa/enforcement/examples/disposalfaqs.pdf

Question:

May a covered entity dispose of protected health information in dumpsters accessible by the public?

Answer:

No, unless the protected health information (PHI) has been rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster. In general, a covered entity may not dispose of PHI in paper records, labeled prescription bottles, hospital identification bracelets, PHI on electronic media, or other forms of PHI in dumpsters, recycling bins, garbage cans, or other trash receptacles generally accessible by the public or other unauthorized persons. The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, in any form, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. Depositing PHI in a trash receptacle generally accessible by the public or other unauthorized persons is not an appropriate privacy or security safeguard. Instead, covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

For example, depending on the circumstances, proper disposal methods may include (but are not limited to):

- Shredding or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
- Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- In justifiable cases, based on the size and the type of the covered entity, and the nature of the PHI, depositing PHI in locked dumpsters that are accessible only by authorized persons, such as appropriate refuse workers.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more information on proper disposal of electronic PHI, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.