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.

First Civil Monetary Penalty, $4.3 million Imposed by Health and Human Services for Violations of the HIPAA Privacy Rule

News Release From the HHS Press Office February 22, 2011

The U.S. Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR) has issued a Notice of Final Determination finding that Cignet Health of Prince George’s County, Md., (Cignet) violated the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS has imposed a civil money penalty (CMP) of $4.3 million for the violations, representing the first CMP issued by the Department for a covered entity’s violations of the HIPAA Privacy Rule.

The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

“Ensuring that Americans’ health information privacy is protected is vital to our health care system and a priority of this Administration. The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule,” said HHS Secretary Kathleen Sebelius.

In a Notice of Proposed Determination issued Oct. 20, 2010, OCR found that Cignet violated 41 patients’ rights by denying them access to their medical records when requested between September 2008 and October 2009. These patients individually filed complaints with OCR, initiating investigations of each complaint. The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient’s request. The CMP for these violations is $1.3 million.

During the investigations, Cignet refused to respond to OCR’s demands to produce the records. Additionally, Cignet failed to cooperate with OCR’s investigations of the complaints and produce the records in response to OCR’s subpoena. OCR filed a petition to enforce its subpoena in United States District Court and obtained a default judgment against Cignet on March 30, 2010. On April 7, 2010, Cignet produced the medical records to OCR, but otherwise made no efforts to resolve the complaints through informal means.

OCR also found that Cignet failed to cooperate with OCR’s investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that the failure to cooperate was due to Cignet’s willful neglect to comply with the Privacy Rule. Covered entities are required under law to cooperate with the Department’s investigations. The CMP for these violations is $3 million.

“Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records, and adhere closely to all of HIPAA’s requirements,” said OCR Director Georgina Verdugo. “The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules.”

Individuals who believe that a covered entity has violated their (or someone else’s) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

A copy of the Notice of Proposed Determination and Notice of Final Determination can be found at http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html. Additional information about OCR’s enforcement activities can be found at http://www.hhs.gov/ocr.

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
The IRS regularly issues alerts about fraudulent use of its name or logo by Internet scam artists. The IRS website says that it never initiates taxpayer communications through e-mail.

The IRS recommends the following techniques to avoid becoming a victim of phishing scams:

- Be skeptical of communications you receive from sources you are not expecting. Verify the authenticity of phone calls, standard mail, faxes or e-mails of questionable origin before responding.

- Do not reveal secret passwords, PINs, or other security-based data to third parties: genuine organizations or institutions do not need your secret data for ordinary business transactions.

- Do not click on links contained in possibly questionable e-mails; instead, go directly to the site already know to be genuine. For example, the only address for the IRS Web site is www.irs.gov—any other variations on this will not lead to the legitimate IRS Web site.

- Do not open attachments to e-mails of possibly questionable origin, since they may contain viruses that will infect your computer and send your personal information to third parties.

- Shred paper documents containing private financial information before discarding.

If you have any doubts about whether a message from the IRS is authentic, the IRS recommends calling 1-800-829-1040 to confirm it. You can send suspicious e-mails or forward links to suspicious websites to phishing@irs.gov.

To learn more about what to do if you receive a suspicious IRS-related communication, visit the IRS website at: http://www.irs.gov/privacy/article/0,,id=179820,00.html?portlet=1

New Data Handling Educational Resources Available

From the Secure Purdue Newsletter-December 2010

How the University handles the vast amounts of data entrusted to it continues to be something that every Purdue employee is interested in. The Purdue University Data Stewards Organization has recently created an Educational Resources webpage. The new webpage features new and revised data handling training resources. The newest resources include a data handling power point presentation and an updated version of the “Keys to Securing Purdue’s Data” pamphlet.

http://www.purdue.edu/securePurdue/policies/dataStewards.cfm

http://www.purdue.edu/securePurdue/procedures/dataClassif/Resources.cfm