HIPAA Privacy & Security Updates—From Dorothy Cociu, COIN Editor and HIPAA Privacy & Security Consultant & Trainer

January, 2017

NEW GUIDANCE ON HIPAA & FTC ACT; UMASS BREACH; HHS/OCR VICTIM OF PHISHING SCAM REGARDING THEIR AUDIT PROGRAM

New Guidance was released on October 21, 2016 for HIPAA and the FTC Act. If your organization shares consumer health information, you must comply with not only HIPAA< but also the Federal Trade Commission Act. Your disclosure statements should also comply with the FTC Act. You can find the new guidance at https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act .

On November 22, 2016, it was reported that The University of Amherst (UMass) agreed to settle potential violations of HIPAA's Privacy & Security Rules. The settlement includes a corrective action plan and a monetary payment of $650,000, which is reflective of the fact that the University operated at a financial loss in 2015 (i.e, if they had made a profit, the penalty would have been higher).

On June 18, 2013, UMass reported to HHS/OCR that a workstation in its Center for Language, Speech, and Hearing (the "Center") was infected with a malware program, which resulted in the impermissible disclosure of electronic PHI (ePHII) of 1,670 individuals, including names, addresses, SSNs, DOBs, health insurance information, diagnoses and procedure codes. The University determined that the malware was a generic remote access Trojan that infiltrated their system, providing impermissible access to ePHI, because UMass did not have a firewall in place.

OCR's investigation indicated several potential violations, including: 1) failure to designate all of its health care components when hybridizing, incorrectly determining that while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components. Because UMass failed to designate the Center as a health care component, UMass did not implement policies and procedures at the Center to ensure compliance with the HIPAA Privacy & Security Rules; 2) UMass failed to implement technical security measures at the Center to guard against unauthorized access to ePHI transmitted over an electronic communications network by ensuring firewalls were in place; 3) UMass did not conduct an accurate and thorough risk analysis until September, 2015.

In addition to the monetary settlement, UMass agreed to a corrective action plan that requires the organization to conduct enterprise-wide risk analysis; develop and implement a risk management plan; revise its policies and procedures, and train its staff on these P&Ps.

On November 28, 2016, HHS/OCR issued an Alert, notifying entities that phishing email disguised as official OCR audit communication was being circulated on mock HHS departmental letterhead under the signature of OCR's director, Jocelyn Samuels. The email targets employees of HIPAA covered entities and their business associates.

The email prompts recipients to click on a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services.

HHS/OCR alerted entities that in no way is this firm associated with the US Department of Health and Human Services or the Office for Civil Rights.

On November 30, 2016, additional clarification was released regarding the incident and audits of Business Associates.

A listserv announcement warning covered entities and their business associates about a phishing email that disguises itself as an official communication from the department. OCR wanted to further share that this phishing email originates from the email address OSOCRAudit@hhs-gov.us and directs individuals to a URL at http://www.hhs-gov.us. *This is a subtle difference from the official email address of the HIPAA Audit Program,* OSOCRAudit@hhs.gov, *but is typical in phishing scams.*

HHS/OCR stated that covered entities and business associates should alert their employees of this issue and take note that official communications from the HIPAA Audit Program are sent to selected auditees from the email address OSOCRAudit@hhs.gov.

More updates will appear in the next issue of the COIN. ##