Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center

The University of Mississippi Medical Center (UMMC) has agreed to settle multiple alleged violations of the Health Insurance Portability and Accountability Act (HIPAA) with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). OCR’s investigation of UMMC was triggered by a breach of unsecured electronic protected health information (“ePHI”) affecting approximately 10,000 individuals. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight. UMMC will pay a penalty of $2,750,000 and adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

“In addition to identifying risks and vulnerabilities to their ePHI, entities must also implement reasonable and appropriate safeguards to address them within an appropriate time frame,” said OCR Director Jocelyn Samuels. “We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI.”

On March 21, 2013, OCR was notified of a breach after UMMC’s privacy officer discovered that a password-protected laptop was missing from UMMC’s Medical Intensive Care Unit (MICU). UMMC’s investigation concluded that it had likely been stolen by a visitor to the MICU who had inquired about borrowing one of the laptops. OCR’s investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC’s wireless network because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008.

Further, OCR’s investigation revealed that UMMC failed to:

- implement its policies and procedures to prevent, detect, contain, and correct security violations;
- implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI; and
- notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

University of Mississippi is the state’s sole public academic health science center with education and research functions. In addition it provides patient care in four specialized hospitals on the Jackson campus and at clinics throughout Jackson and the state. Its designated health care component, UMMC, includes University Hospital, the site of the breach in this case, located on the main UMMC campus in Jackson.
FOR IMMEDIATE RELEASE
July 18, 2016
Contact: OCR Press Office
202-619-0403
media@hhs.gov

Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University

Oregon Health & Science University (OHSU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules following an investigation by the U.S. Department of Health and Human Services Office for Civil Rights (OCR) that found widespread and diverse problems at OHSU, which will be addressed through a comprehensive three-year corrective action plan. The settlement includes a monetary payment by OHSU to the Department for $2,700,000.

OCR’s investigation began after OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. These incidents each garnered significant local and national press coverage. OCR’s investigation uncovered evidence of widespread vulnerabilities within OHSU’s HIPAA compliance program, including the storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a business associate agreement. OCR found significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses.

OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but OCR’s investigation found that these analyses did not cover all ePHI in OHSU’s enterprise, as required by the Security Rule. While the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, OHSU did not act in a timely manner to implement measures to address these documented risks and vulnerabilities to a reasonable and appropriate level. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk.

“From well-publicized large scale breaches and findings in their own risk analyses, OHSU had every opportunity to address security management processes that were insufficient. Furthermore, OHSU should have addressed the lack of a business associate agreement before allowing a vendor to store ePHI,” said OCR Director Jocelyn Samuels. “This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously.”

OHSU is a large public academic health center and research university centered in Portland, Oregon, comprising two hospitals, and multiple general and specialty clinics throughout Portland and throughout the State of Oregon.