BULLETIN – July 10, 2015

HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications

St. Elizabeth's Medical Center (SEMC) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). SEMC will pay $218,400 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. SEMC is a tertiary care hospital located in Brighton, Massachusetts that offers both inpatient and outpatient services.

On November 16, 2012, OCR received a complaint alleging noncompliance with the HIPAA Rules by SEMC workforce members. Specifically, the complaint alleged that workforce members used an internet-based document sharing application to store documents containing electronic protected health information (ePHI) of at least 498 individuals without having analyzed the risks associated with such a practice. Additionally, OCR's investigation determined that SEMC failed to timely identify and respond to the known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome. Separately, on August 25, 2014, SEMC submitted notification to HHS OCR regarding a breach of unsecured ePHI stored on a former SEMC workforce member's personal laptop and USB flash drive, affecting 595 individuals.

"Organizations must pay particular attention to HIPAA's requirements when using internet-based document sharing applications," said OCR Director Jocelyn Samuels. "In order to reduce potential risks and vulnerabilities, all workforce members must follow all policies and procedures, and entities must ensure that incidents are reported and mitigated in a timely manner."

In addition to the $218,400 settlement amount, which takes into consideration the circumstances of the complaint and breach, the size of the entity, and the type of PHI disclosed, the agreement includes a corrective action plan to cure gaps in the organization's HIPAA compliance program raised by both the complaint and the breach. The Resolution Agreement can be found on the OCR website at: www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/ra.pdf

For guidance on how your organization can meet privacy and security responsibilities, click here: www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights, and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.hhs.gov/ocr/office

Follow us on Twitter @HHSOCR.

###