Long-Term Care Survey Alert

Privacy: OCR Enforces Huge Fine for Privacy Breach

MEEI to pay HHS $1.5 million to settle potential HIPAA violations.

The **U.S. Department of Health and Human Services' Office for Civil Rights** (OCR) is showing that it intends to treat even potential HIPAA violations as gravely as it treats actual data security breaches.

"**Massachusetts Eye and Ear Infirmary** (MEEI) and **Massachusetts Eye and Ear Associates, Inc.** (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services' (HHS) $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule," the HHS announced in a Sept. 17 press release.

MEEI had earlier reported the theft of an unencrypted personal laptop containing the electronic protected health information (ePHI), including prescriptions and clinical information, of MEEI patients and research subjects. It "also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information," the release added.

"Necessary steps to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices, implementing security measures sufficient to ensure the confidentiality of ePHI that MEEI created, maintained, and transmitted using portable devices," were not taken by MEEI according to the OCR investigations.

Background: In June, the **Alaska Department of Health and Social Services** (DHSS) was fined $1,700,000 by the HHS for possible HIPAA violations when DHSS had reported that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of an employee.

"The evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule," the June 26 HHS press release had announced.

"Covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices," OCR Director **Leon Rodriguez** was quoted as saying in the same release. "This is OCR's first HIPAA enforcement action against a state agency and we expect organizations to comply with their obligations under these rules regardless of whether they are private or public entities."

Reminder: Entities covered by HIPAA are required by the HIPAA security rule to use physical, technical and administrative safeguards to ensure that electronic protected health information remains private and secure.