# Health Information Compliance Alert

## Protect Yourself: Mobile & Medical Devices Are Ripe For HIPAA Breaches

**Know what specific policies and procedures the OCR is looking for you to have in place.**

Hackers seem to always find new ways of accessing private information, especially when it comes to electronic protected health information (ePHI), and one trend that's gaining steam is theft of ePHI via medical devices and related radiological equipment. Unfortunately, this type of breach can cost you hundreds of thousands of dollars or more  here's how one healthcare provider learned this lesson the hard way.

**Background:** In August 2011, a laptop was stolen from an unlocked treatment room at **Lahey Hospital and Medical Center**, a nonprofit teaching hospital affiliated with **Tufts Medical School** in Burlington, Mass., according to a Nov. 25 **HHS Office for Civil Rights** (OCR) announcement. The laptop was on a stand that accompanied a portable CT scanner, and the laptop operated the scanner, producing radiological images.

The laptop hard drive contained the PHI of 599 individuals. Lahey notified OCR of the theft and resulting HIPAA breach, and then OCR conducted an investigation.

**Don't Make the Same Mistakes**

**Red flags:** OCR's investigation revealed "widespread noncompliance with the HIPAA Rules," according to the announcement. Specifically, OCR found that Lahey:

- Failed to conduct a thorough risk analysis of all its electronic PHI (ePHI);
- Did not physically safeguard a workstation that accessed ePHI;
- Neglected to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
- Did not enforce the use of unique user names for identifying and tracking user identity with respect to the workstation at issue in the incident;
- Failed to implement procedures that recorded and examined activity in the workstation at issue; and
- Subsequently caused the impermissible disclosure of 599 individuals' PHI.

In the settlement that OCR announced on Nov. 25, Lahey must pay $850,000 and adopt a "robust" Corrective Action Plan (CAP) to "address its history of noncompliance with the HIPAA Rules." Lahey must provide OCR with a comprehensive, enterprise-wide risk analysis and corresponding risk management plan, as well as report certain events and provide evidence of compliance.

**What Compliance Looks Like to OCR**

**Insight:** Unfortunately, Lahey's case is not unique  a Dec. 1 analysis by attorneys **Elizabeth Hodge** and **Thomas Range of Akerman LLP** pointed to **Cancer care Group, P.C.**'s recent settlement agreement, which involved the theft of unencrypted computer server backup media and yielded similar "robust" requirements in its CAP (see "Backup Devices: Learn 3 Crucial Lessons From The Latest Data Breaches," HICA, Vol. 15, No. 9, page 65).

These cases "demonstrate the OCR's focus on the importance of risk analysis and device and media control policies," Hodge and Range cautioned. And in response, the CAP requires Lahey to:

- Conduct an **organization-wide risk analysis** of its electronic media, workstations, and information systems and develop a risk management plan to address the risks and vulnerabilities that the risk analysis identifies. Lahey

must submit its risk analysis methodology and risk management plan to OCR for approval.

- Develop or revise its **written policies and procedures** to address compliance failures underlying the breach. OCR must pre-approve these policies and procedures, which must include procedures for:
- Recording the receipt, removal, and disposition (whether external or internal to Lahey's facility) of hardware and electronic media that maintain ePHI;
- Ensuring workstations that maintain ePHI used in connection with diagnostic or laboratory equipment are registered with, and under the control of, Lahey's Information Services Department; and
- Implementing mechanisms that record and examine activity in information systems of workstations that maintain ePHI used in connection with diagnostic or laboratory equipment.
- Promptly report to OCR any **workforce failures** to comply with its policies and procedures.
- Submit to OCR an **implementation report** that includes an attestation by an officer of the hospital that Lahey has implemented the policies and procedures, as well as an attestation by a hospital officer that, based on the officer's review of the implementation report and reasonable inquiry regarding its content, the officer believes the information is accurate and truthful.

**Take These Actions Now**

Additionally, Hodge and Range advised that you review these OCR settlement agreements to determine whether your policies and procedures adequately address device security in the OCR's eyes. Also, do you need to update your organization's risk analysis due to new risks involving devices that the OCR, the **Food and Drug Administration** (FDA), and other government agencies have identified, such as hackers' ability to infiltrate hospital systems through medical devices?

**Crucial:** Is your risk management plan current? Do you need new policies and procedures to address newly identified risks and vulnerabilities associated with mobile and medical devices? And finally, are your workforce members who access ePHI current with their HIPAA training requirements? The OCR is clearly looking for providers to be compliant with all of these requirements.

**Resources:** To read the OCR's Resolution Agreement and CAP with Lahey, go to www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/Lahey.html. A guidance document on how to protect and secure ePHI when using mobile devices is available at www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.