# PUBLICATION

## $1.5 Million OCR HIPAA Settlement Provides Notice of Increased Enforcement Focus on Mobile Device Security and Encryption [Ober|Kaler]

**September 28, 2012**

***Bloomberg BNA Health IT Law & Industry Report***

***Reproduced with permission from* Health IT Law & Industry Report**

**The HHS Office of Civil Rights (OCR) recently announced a $1.5 million dollar settlement with a Massachusetts specialty hospital and its associated professional group practice following a lengthy investigation of the entities' (collectively, "Massachusetts Eye and Ear Infirmary," or "MEEI") HIPAA privacy and security practices. MEEI has publicly expressed its disappointment with the size of the monetary settlement. In addition to the monetary settlement (which will be spread over three years) MEEI was required to execute a three-year Corrective Action Plan (CAP) that requires the use of an outside Monitor, semi-annual inspections, and the production of implementation, annual, and semi-annual Monitor reports.**

MEEI's troubles began on Feb. 19, 2010, when Dr. Robert Levine's laptop was stolen during a lecture tour in South Korea. The stolen laptop contained demographic and health information of approximately 3,526 patients treated by Dr. Levine at Mass. Eye and Ear between Feb. 3, 1988, and Feb.16, 2010, as well as information concerning a small number of research participants who were not patients of Dr. Levine. MEEI performed an investigation, and, on April 20, 2010, issued a press release concerning the breach. MEEI also, in keeping with all of its legal obligations, notified all affected individuals, as well as OCR.

As has been the case with all breaches involving more than 500 individuals, OCR opened an investigation into MEEI's HIPAA compliance. According to the most recent MEEI press release, that investigation was ongoing since MEEI's initial report of the laptop theft. MEEI's press release states that it was cooperative during all phases of the investigation and made all compliance adjustments suggested and corrected all deficiencies noted by OCR investigators.

Nevertheless, OCR apparently determined that both a monetary penalty and the imposition of a CAP were necessary, a conclusion that MEEI disputes.

## MEEI's Violations

OCR's Resolution Agreement (RA) (which also attaches a copy of the CAP) provides some detail regarding the categories of non-compliance it identified as justifying the monetary settlement and CAP:

- MEEI did not "demonstrate that it conducted a thorough analysis of the risk to the confidentiality of ePHI on an on-going basis as part of its security management process from the compliance date of the Security Rule to Oct. 29, 2009." More specifically, MEEI did not sufficiently assess the risks posed by mobile devices, did not take sufficient steps to ameliorate those risks, and did not sufficiently document the security steps it chose (and why it chose them) or update those steps on a regular enough basis.

- MEEI's security measures for mobile devices were not at a "reasonable and appropriate level."
- MEEI lacked adequate policies and procedures for identifying, reporting, and responding to data breaches.
- MEEI lacked adequate policies governing the use of portable devices to store or transmit PHI. Notably, the RA specifically notes that "MEEI had no reasonable means of tracking non-MEEI owned portable media devices containing its ePHI into and out of its facility, or the movement of these devices within the facility."
- MEEI failed to implement adequate technical policies to "allow access to ePHI using portable devices only to authorized persons or software programs. . ." nor did it "implement an equivalent, reasonable, and appropriate alternative measure to encryption . . . or document the rationale supporting the decision not to encrypt."

The RA does not provide, of course, an explanation of the steps that MEEI had taken, making it very difficult to determine whether MEEI's privacy and security protocols were truly obviously and unreasonably deficient or whether MEEI (like many other providers) had in place what they believed to be perfectly adequate policies and procedures.

Similarly, the listing of violations does not cite to any specific regulation or standard to support its determination that a violation has occurred (mostly because the standards at work, "reasonableness," "appropriateness," and "sufficiency" are not specifically defined in any regulation or guidance).

As discussed below, however, the violations cited by OCR reveal a great deal about what the government is likely to find "reasonable" in the context of mobile devices containing PHI.

## MEEI's CAP

As we have discussed in other articles, a settlement with OCR generally requires not only a cash payment but also a commitment to a (generally, and in this case, three year) Corrective Action Plan. These plans are intended to ensure ongoing compliance much in the same fashion as Corporate Integrity Agreements are intended to ensure ongoing compliance following a settlement with the HHS Office of Inspector General. The two agreements also share a tendency to burden provider's with significant ongoing reporting and auditing responsibilities as well as substantial costs related to a diversion of enterprise resources and the retention of (and satisfaction of) an outside auditor. MEEI's CAP is a fairly typical example, including:

- The creation of all new policies and procedures, which must be submitted to HHS for edits and approval;
- The distribution of the new policies and procedures, including the collection of signed certifications from all MEEI workforce members;
- Training of all workforce members (also requiring signed certifications from all workforce members, as well as the submission of all training materials);
- The retention of an independent Monitor (approved by HHS);
- The creation of a "Monitor Plan" detailing the responsibilities of the Monitor, which shall include, at a minimum;

    - Twice yearly unannounced site inspections (which will include both document reviews and workforce interviews);
    - Twice yearly written reports to HHS;
    - Immediate reporting of all "significant noncompliance;" and

  - Provision for a "validation review" (essentially, providing HHS OCR the right to conduct its own investigation in the event it believes the monitor has not properly performed its duties).
- The reporting of all events of non-compliance (reportable events) following an internal investigation by MEEI to both HHS and the Monitor;
- The creation of an "implementation report" describing the steps taken to implement required steps of the CAP, to be submitted to HHS and the Monitor (along with a signed attestation as to its accuracy;
- The creation and submission of attested Annual Reports, to be submitted to both HHS and the Monitor; and
- The retention of all documents "relating to compliance with the CAP" for six years.

In the event that MEEI fails to fulfill its responsibilities under the CAP, it is subject not only to an additional investigation and any penalties resulting from the conduct that breached the CAP, but, HHS OCR is no longer bound by its release of MEEI for the conduct originally giving rise to the settlement.

Needless to say, compliance with the detailed three year CAP will add significantly to the costs incurred as a result of the theft of Dr. Levine's laptop.

## Comments

OCR's settlement with MEEI is instructive in several ways to any provider, but especially those providers who allow workforce members to use portable media to transport or store ePHI.

- Encryption is a *must*: Although neither the Security Rule nor any guidance interpreting it have made encryption mandatory (it is an "addressable standard under the Security Rule, i.e. if it is not adopted a reason must be documented and an appropriate alternative measure must be justified and applied) providers who use portable media simply MUST encrypt those devices. If the MEEI resolution is any indication, the OCR will set a high standard for any alternative to encryption of a portable device containing PHI. If providers intend to reach that bar and use an alternative to encryption, they must clearly document what is used, how it is equivalent, and why encryption was not possible.
- The covered entity (not the workforce member) should own and control the portable device/media. Although it has become popular in these difficult economic times to permit workforce members to utilize their own portable devices (laptops, phones, flash drives, etc), permitting ePHI to spread onto media that can be neither controlled nor monitored by the organization is clearly unacceptable to OCR. Best provider practices will include the provision of dedicated, enterprise controlled devices where necessary. Barring that, providers should ensure that their system allows workforce members to access and download only the minimum necessary ePHI and that all such downloads (including all downloaded ePHI) are reviewable in system logs.
- Policies, Procedures, and Training regarding the use of mobile devices and portable storage media are *required*. These additions to every organizations' policies and procedures should be detailed, and all training should be well documented. Loss of portable devices is rapidly becoming the most popular way to draw the attention of HHS OCR, and it is a problem that can be best addressed through a combination of technological safeguards (encryption, access limits, remote-wipe capabilities, and access log monitoring) and human intelligence (do not leave your laptop on your car seat in plain view—even for a moment.)
- Similarly, covered entities must ensure their policies and procedures (and their training) include clear directions to all workforce members on what constitutes a breach, who should be contacted (even on nights and weekends) and what steps should be taken immediately to ensure all data breaches are properly reported and addressed promptly.

- Finally, providers should note that, when it comes to HHS OCR, no news is not necessarily good news. By statute, OCR must post a notice regarding all breaches affecting 500 or more individuals—it posts them on this dedicated web page. It is not a short list. By policy, OCR has investigated (or will investigate) all of these large breaches. That a breach occurred two (or more) years ago clearly does not mean that OCR has elected to "let this one slide." Providers who experience a breach involving more than 500 individuals' PHI should expect an investigation and should be prepared to demonstrate the steps they have taken both before and since to ensure and where necessary improve compliance.