# PUBLICATION

## HIPAA Settlement Regarding Use of Internet Applications

**Authors: Alisa L. Chestler**
**July 14, 2015**

On July 10, 2015, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced a settlement agreement with St. Elizabeth's Medical Center (SEMC) in Brighton, Massachusetts, regarding potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules. SEMC has agreed to pay OCR $218,400 and must adopt a corrective action plan to correct deficiencies in its HIPAA compliance program.

The original complaint to OCR was made by a workforce member on November 16, 2012, and OCR notified SEMC of its investigation on February 14, 2013. 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. It is significant to note that the Resolution Agreement does not allege any improper disclosure to any outside entity or person – the violation appears to be focused on the failure to review the practice as a part of a security risk analysis and 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 notified OCR regarding a breach of unsecured ePHI stored on a former SEMC workforce member's personal laptop and USB flash drive, affecting 595 individuals.

The Resolution Agreement includes a corrective action plan (CAP) to cure gaps in SEMC's HIPAA compliance. Included in the CAP is a specific obligation to educate workforce members on policies and procedures which address (1) transmitting ePHI over unauthorized networks; (2) storing ePHI on unauthorized information systems, including unsecured networks and devices; (3) removal of ePHI from SEMC; (4) prohibition of shared accounts and passwords for ePHI access or storage; (5) encryption of portable devices that access or store ePHI and (6) security incident reporting related to ePHI. All covered entities and business associates should review their current policies and procedures to determine if such issues are covered and potentially amend their training to inform workforce members of such policies and procedures.

The CAP also includes a robust self-assessment reporting requirement which is due to OCR within 150 days of the settlement. The self-assessment requirements include: (1) unannounced site visits to five SEMC departments, including the Cardiology Department (the "Covered Department") to assess implementation of the policies and procedures; (2) interviews with a total of 15 randomly selected SEMC workforce members who have access to ePHI, 13 of whom shall be from the Covered Departments – including at least one intern, resident, or fellow, and the remaining two of whom shall be interns, residents, or fellows working in Hematology/Oncology; and (3) inspection of at least three portable devices at each of the Covered Departments that can access ePHI, including one laptop, one other portable device, such as a tablet or smartphone, and one portable storage media, such as a USB flash drive, randomly selected to ensure that such devices satisfy all applicable requirements of the policies and procedures.

The CAP contains several other significant sections which merit review and consideration, including a fairly robust reporting requirement of all investigations of workforce members who have violated policies and procedures.

The Resolution Agreement can be found on the OCR website here.

OCR also used the opportunity to remind organizations of the recent updated publication from the Office of the National Coordinator designed to assist all organizations with considerations related to their compliance programs. The guide can be found here.

For more information about how this settlement may affect your business, or related matters, contact the author of this alert, Alisa L. Chestler, or any members of the Firm's Privacy and Information Security Team.