

**From:** [Raines, Jill \(HSC\)](#)  
**To:**

**Subject:** New \$5.5M Settlement for HIPAA Violations - Please Read  
**Date:** Friday, February 17, 2017 9:11:23 AM

---

Good morning Health Care Component Contacts and HCC Business Administrators –

Yesterday, the Office for Civil Rights announced a \$5.5M HIPAA settlement with a non-profit healthcare system. The settlement was, in part, for violations related to a former employee's log-in credentials being used to access PHI after the employee's separation from the healthcare system. The University has several measures in place to protect patient and research participant PHI from unauthorized access after a workforce member leaves his or her position, and those measures rely heavily on actions to be taken by clinic and department managers and their staff.

Please review the announcement below and remind appropriate workforce members to take the following steps for each separation:

1. Complete the Termination/Property Clearance Checklist process, which requires
  - a. Return of all keys and badges (ID, building entry, proximity/tap, etc.)
  - b. Disabling of all access to University systems (email, EMR/billing, building access, etc.), generally *at the time of separation*
2. Update the Role-Based Access Worksheet to reflect the separation and change in access. (Don't forget to update this document during employment as well, each time access rights to PHI change.)

**Please DO NOT ASSUME that someone else is taking care of these steps for your area.** If you have not already done so, please document who in your area will ensure that all badges and keys are collected, that 1Call and Access Control (HSC) or Sooner Card (Norman) or HR (Tulsa) is notified to terminate building access, that IT is contacted to close email accounts, and that the EMR team is asked to remove access to electronic medical and billing systems. Know who is completing each item on the Checklist to ensure no steps are missed in your area.

Thank you for your help with the University's HIPAA compliance program. If you have any questions, please contact me or Marty Walton at 271-2033, Mary Milano (HIPAA Compliance Auditor) at 271-6674 , or Valerie Golden (HIPAA Security Officer) at 271-8001 x 46456.

*Jill Bush Raines*

Assistant General Counsel and

University Privacy Official

University of Oklahoma

(405) 271-2033 / 271-1076 fax

May contain privileged or confidential information; may not be shared without permission.

**February 16, 2017**

**\$5.5 million HIPAA Settlement**

**Memorial Healthcare Systems (MHS)** has paid the U.S. Department of Health and Human Services (HHS) **\$5.5 million** to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and agreed to implement a robust corrective action plan. MHS is a **nonprofit corporation** which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS **failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access**, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

The Resolution Agreement and Corrective Action Plan may be found on the OCR website at <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial>