To: All OUHSC Faculty, Staff, Residents, and Fellows September 14, 2015
From: Jason R. Sanders, MD, MBA
Interim Senior Vice President and Provost

IMPORTANT PLEASE READ: Update to the OUHSC Laptop Encryption Process

This memo updates the process by which the laptop encryption policy is being implemented on the OUHSC campuses. The current laptop encryption policy, adopted in October 2013, states, "**ALL laptops used for University business must be encrypted, regardless of who owns the laptop, or the operating system…"** See Portable Computing Device Security at http://it.ouhsc.edu/policies/PortableDeviceSecurityPolicy.asp

Thank you for your cooperation.

Current Status of the Encryption Process:

Phase I to encrypt all University-owned MS Windows laptops started in 2013. Phase I is complete and has prevented several data breaches.

However we continue to have data breaches from lost or stolen **personally-owned** MS Windows and Macintosh laptops. **We must continue the process to encrypt ALL laptops used for University business—this includes personally-owned as well as University-owned laptops**.

Next Steps in the Mandatory Encryption Process: IMPORTANT---PLEASE READ

Phase II effective September 2015, for all **College of Medicine residents and fellows**: **All personally-owned or University owned Macintosh and MS Windows laptops used for University business must be encrypted by the department Tier 1**. The Tier 1 will install an agent on the laptop that communicates with a security management server to provide centralized reporting required for regulatory compliance. Residency and Fellowship Program Directors will receive instructions on the process to encrypt residents' and fellows' laptops. (The OU Tulsa School of Community Medicine does not allow residents or fellows to use their personally-owned laptops for university business.)

Phase III for **all OUHSC faculty and staff**: **All laptops used for University business must be encrypted by the department Tier 1**. This includes personally-owned laptops with MS Windows or Macintosh operating systems. Details of the process will be provided to faculty and staff by their department Tier 1 in the next few weeks.

Liability: It is incumbent upon all employees of the University to take steps to protect ALL University data on ALL laptops, thus ensuring sensitive and regulated data is protected. **Under Federal law, employees may be held personally responsible for the loss of an unencrypted device that contains electronic Protected Health Information (ePHI), including large fines and up to 10 years imprisonment**.

HIPAA enforcement and penalties for the loss or theft of unencrypted ePHI are increasing. Millions of dollars in penalties have been assessed against health care organizations for the loss or theft of

unencrypted devices. http://www.healthcareinfosecurity.com/another-big-fine-after-small-breach-a-5116.

What Should You Do?

PHI may NOT be stored on unencrypted laptops.

University employees must take all required, reasonable, and prudent actions necessary to ensure the security and retention of sensitive University data. University employees **SHALL** maintain up-to-date, device-appropriate security safeguards and follow the policies, standards, and guidance provided by the University, as well as comply with appropriate safeguards required by state and federal regulations.

Incident reporting: All devices, including personally-owned devices, that access or maintain sensitive University data and that are lost, stolen, have been subject to unauthorized access, or otherwise compromised must be reported immediately to Campus Police, IT Security, and the HIPAA Privacy Official.

Definitions

University business: Work performed as part of an employee's job responsibilities, or work performed on behalf of the University by faculty, staff, volunteers, students, other trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. In the context of laptop use, University business includes the use of a laptop to access OUHSC email, non-public University systems, networks, or data in the performance of work for the University.

Sensitive University data: Any information, which through loss, unauthorized access, or modification could adversely affect any of the missions of the University or the privacy of individuals. Some sensitive data is protected by law or regulation, while other data is determined to be sensitive by virtue of its importance to the mission of the University. Examples of sensitive data include medical and patient information, credit card numbers, Social Security numbers, financial records, student records, employee data, and research data.