From: Andrews, Dewayne (HSC)
Sent: Monday, October 21, 2013 9:34 AM
To: HSC-OUHSC
Subject: Clarification of Laptop Encryption Policy & Process
Importance: High

October 2013

IMPORTANT: Clarification of OUHSC Laptop Encryption Policy and Process

This memo clarifies the process by which the laptop encryption policy will be implemented on the OUHSC campuses. The policy states, "ALL laptops used for University business must be encrypted, regardless of who owns the laptop, or the operating system (MS Windows or Apple Macintosh) used."

Current Status of the Encryption Process: Since the laptop encryption policy was adopted, there have been concerns raised regarding the difficulty of complying with immediate and full-scale implementation of the mandated encryption on all laptops, as well as requests by departments for clarification of the policy. These concerns and requests relate primarily to the use of personally-owned laptops used for University work and to identifying a suitable technology solution to address Macintosh encryption issues that have surfaced. It has become clear that a phased implementation is necessary.

Next Steps in the Encryption Process: Our goal remains the same: protect ALL University data on ALL laptops from the threat of compromise when a laptop is lost or stolen. For practical reasons, implementing encryption on the variety of laptops used by University faculty, staff, students and other workforce members requires multiple phases based upon the type of laptop hardware, software, and ownership. The process has started with University-owned MS Windows laptops which is almost complete and will continue towards encryption of all University-owned Mac laptops, followed by those personally-owned MS or Mac laptops used for University business. Phases are as follows:

Phase 1-- Mandatory encryption of **University-owned MS Windows laptops** is 90% complete. Over 1,850 laptops have been successfully encrypted.

Phase 2-- Encryption of **University-owned Macintosh laptops** –Strongly encouraged but not yet mandatory. This is taking place in numerous departments. Before a campus-wide implementation is mandatory, IT will complete testing of a new solution to address performance issues encountered with some Mac laptops and encryption.

Phase 3-- Encryption of **Personally-owned MS Windows** and **Personally-owned Macintosh laptops**— Strongly encouraged but not yet mandatory. This has started within a few departments and may continue in those areas. However, before becoming mandatory, a multi-campus work group will explore a range of issues related to use of personally-owned laptops for University business.

Security of Personally-Owned Devices that Access Sensitive University Data: [See definitions of portable computing device, University business, and sensitive University data at the end of this memo.]

Sensitive University data shall be accessed or temporarily housed on personally-owned devices **ONLY** when necessary for the performance of University-related duties and activities. As such, when

conducting University activities, it may at times be necessary for University employees, agents, affiliates, or workforce members to access or temporarily house sensitive University data on personally-owned devices. There is often risk of data loss or unauthorized access when sensitive University data is accessed or temporarily housed on self-managed personally-owned devices. **ALL members of the University community who access or temporarily house sensitive University data have a shared obligation and responsibility to secure such data by properly self-managing the privacy and security settings on their personally-owned devices (i.e. password protection, encryption, automated log-off, etc.) and physically securing those devices.** For assistance with this, please contact the IT Service Desk at 271-2203.

University employees must take all required, reasonable, and prudent actions necessary to ensure the security and retention of sensitive University data. University employees, agents, affiliates, and workforce members **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. See Portable Computing Device Security at http://it.ouhsc.edu/policies/PortableDeviceSecurityPolicy.asp

Liability: It is incumbent upon all workforce members 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 in jail**.

HIPAA enforcement and penalties for the loss or theft of unencrypted ePHI are increasing. In recent months, millions of dollars of penalties have been assessed against health care organizations for the loss or theft of unencrypted devices. http://www.healthcareinfosecurity.com/stolen-devices-persistent-problem-a-5133.

Incident reporting: All devices, including personally-owned devices, that access or maintain sensitive institutional data and that are lost, stolen, have been subject to unauthorized access, or otherwise compromised must be reported within 24 hours to Campus Police and IT Security.

What Should You Do?

PHI should NOT be stored on Portable Computing Devices unless absolutely necessary; it should be stored on servers in a secure enterprise data center. Data centers provide data backup and recovery services that can restore data in the event of a hard drive failure or natural disaster. Data stored on a Portable Computing Device will typically be unrecoverable when that device is lost or stolen or the hard drive fails. Therefore, extreme caution must be used in storing PHI on Portable Computing Devices, even on those that are encrypted.

Definitions

Portable Computing Device (PCD): includes but is not limited to notebook computers; tablet PCs; handheld devices such as Portable Digital Assistants (PDAs), iPads; Palm Pilots, Microsoft Pocket PCs,

RIM (Blackberry); smart phones such as iPhones, Androids and MS Windows phones; and converged devices.

University business: work performed as part of your job responsibilities as an employee of the University, or work performed on behalf of the University as faculty, staff, volunteers, students and 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 ("workforce"). In the context of laptop use, University business would include the use of a laptop to access 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 information, credit card numbers, Social Security numbers, financial records, student records, employee data, research data, etc.

Thank you for your cooperation.

M. Dewayne Andrews, M.D.
Senior Vice President and Provost
Executive Dean, College of Medicine