The University of Texas System
Nine Universities. Six Health Institutions. Unlimited Possibilities.

**Office of Health Affairs**
601 Colorado, Austin, TX 78701
Phone: 512-499-4224 Fax: 512-499-4313

June 20, 2012

MEMORANDUM

To: Presidents, The University of Texas System Health Institutions

From: Kenneth I. Shine, M.D., Executive Vice Chancellor for Health Affairs

Subject: Highest Priority- Encryption of all University Laptop Computers

---

After considerable discussion with the leadership of our Board of Regents, we are asking all campuses to encrypt all University laptop computers, including personally owned computers used for any University business. If a faculty or staff person must use a personally owned computer to conduct any University business, including research or health care of any type, the computer must be encrypted by the institution's information security staff. Our target for encryption is 100% of these computers by August 31, 2012.

This is likely to require significant additional resources on some campuses, but we have now had serious problems with loss of unencrypted computers creating costly emergencies. All computers should be included because it is unclear when a given computer has confidential data including patient information. Because this will affect faculty and other high ranking employees, we recommend that you utilize the directors of your patient care and research departments to help communicate this requirement. In June, 2007, The University of Texas System adopted as policy, "Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices" http://utsystem.edu/ciso/SPB1.pdf. Since adoption of the policy, U. T. institutions have avoided a number of serious data exposures due to laptop computers having been encrypted prior to becoming lost or stolen. Unfortunately, during this same period, U. T. institutions have also experienced incidents in which encryption of laptops had not been put in place. Some of these incidents resulted in serious data exposures. Our real-world experience teaches us that laptop encryption cannot be optional. It must be a required security control for all University laptop computers. This is the least expensive, easiest, and most cost effective manner for us to achieve a high degree of security on laptop devices.To ensure timely response and implementation, please provide, no later than July 1, 2012, a report containing: 1) the number of laptop computers owned by the institution, 2) the number of these devices that are currently encrypted, 3) the rate at which laptop computers are being encrypted, and 4) your institutional plan for achieving 100% compliance,, and 5) your plan for ensuring that all personal computers that contain patient, research, or other sensitive data related to University business are also encrypted.

If your institution anticipates that it cannot meet the target date for all laptops, an acceptable alternative is to notify us in your report that all laptops containing patient data or medical records of any kind are encrypted by the target date along with the date that all laptops will be encrypted. If you believe that compelling circumstances will prevent your institution from meeting either of these targets, please report the earliest dates(s) for encrypting high-risk and all laptops along with the circumstances that will prevent earlier compliance. Your report and plan is to be sent by email to kshine@utsystem.edu and copied to ciso@utsystem.edu.

U. T. System will review your plan and will work with you to achieve 100% compliance. A FAQ has been prepared to provide more information and to answer questions. The FAQ is attached to this communication. If you have questions not addressed within the FAQ, please send these to ciso@utsystem.edu or contact Lewis Watkins at (512) 499-4540.

This push to complete encryption of all laptop computers, is phase 1 of a multi-phase process for expanding encryption to eventually include mobile phones, tablet devices, and also desktop computers, and U. T. System policy is being updated to reflect our new regulatory and threat environment. In the coming weeks, you will receive additional information as these plans and timetables are developed.