TEMPLE UNIVERSITY HEALTH SYSTEM
INFORMATION SERVICES & TECHNOLOGY
POLICIES AND PROCEDURES

NUMBER: 0307
TITLE: Removable Storage Encryption Policy
EFFECTIVE DATE: 12-10-2008
LAST REVISED: 03-24-2014
LAST REVIEWED: 03-24-2014
REFERENCES: N/A
ATTACHMENTS: N/A

PURPOSE

Removable storage devices, also known as "flash drives", are useful tools for handling large amounts of data, including patient information. Because of their size, however, they can be easily misplaced or lost, potentially placing significant amounts of electronic Protected Health Information (ePHI) at risk with possible financial and legal harm to TUHS and its patients. The removal of ePHI from a Network (secured with access controls) to a removable storage device requires that the necessary and mitigating controls, i.e., encryption and password protection, exist with the device.

POLICY

Transfer of ePHI to removable storage devices is allowed only when the devices support strong encryption and password protection. TUHS staff who uses "flash drives" or removable storage devices to store ePHI must use secured devices that use at least 256-bit AES (AES-256) encryption and strong password protection.

These devices are to be obtained from Information Services & Technology (IS&T). IS&T will register the devices with users to allow them to write to those devices only. In addition, IS&T uses Network Software controls to prevent unauthorized writing of data to unapproved removable storage devices, and will configure PCs to prevent their booting from CD-ROM or removable storage devices unless a secured password is entered by IS&T technical staff.

Breaches of security related to access are to be reported to the Chief Information Security Officer as soon as noted.

Compliance to Related Standards and Regulations

- NIST Special Publication 800-66 Revision 1, which details recommended HIPAA implementations, references HIPAA Security Rule 164.312(e)(2)(ii), which specifically instructs health care organizations to encrypt electronic Patient Health Information (ePHI) when appropriate. The removal of ePHI from a secured Network to a removable storage device that does not have the protection of TUHS Network access controls is considered an appropriate use of encryption.

- HIPAA Security Rule 164.310(a)(2)(ii) requires TUHS to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. The use of encryption and password protection to protect ePHI, in this case, mitigates these risks.

POLICY APPROVAL PAGE

Recommended by:

Maribel Valentin
Corporate Compliance and Privacy Officer, TUHS
Date:4-01-2014

Mitchell B. Parker
Chief Information Security Officer, TUHS
Date: 4-01-2014

Approved by:

David Kamowski
VP/Chief Information Officer, TUHS
Date: 4-01-2014