# TEMPLE UNIVERSITY HEALTH SYSTEM
# INFORMATION SERVICES AND TECHNOLOGY
# POLICIES AND PROCEDURES

| | |
|---|---|
| **NUMBER:** | TUHS-IS-0307 |
| **TITLE:** | Removable Storage Encryption Policy |
| **EFFECTIVE DATE:** | 12-10-2008 |
| **LAST REVISED:** | 5-23-2019 |
| **LAST REVIEWED:** | 8-11-2021 |
| **REFERENCES:** | TUHS-IS-0511-Epic Report Access_Share_Export Policy |
| **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 transfer of ePHI to a removable storage device requires that the necessary mitigating controls, encryption and password protection, are in place.

## POLICY

When transferring of ePHI to removable storage devices is allowed, TUHS staff shall only use devices that support strong encryption and password protection. TUHS staff who use "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 uses Network Software controls to prevent unauthorized writing of data to unapproved removable storage devices on clinical auto-login devices, IS&T configures PCs with Bitlocker 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 they are discovered.

Compliance to Related Standards and Regulations

- 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

**Recommended by:**

8/11/21

Stephen Felicetti
Sr. Information Security Engineer
Temple University Health System

Date Signed

**Approved by:**

8/18/2021

Deborah Cancilla
EVP Data Strategy / CIO
Temple University Health System

Date Signed

*NOTE:*

***Refer to the on-line version of this policy for the most current information. Printed copies of this policy may not be current.***

***Use of this document is limited to Temple University Health System staff only. It is not to be copies or distributed outside of the institution without Administrative permission.***