POLICY INFORMATION

Document # **4000**	Title: **Device and Media Controls**	Print Date: **8/15/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Physical**	Approved by: **Dean Beth E. Foley** DocuSigned by: Beth Foley 7AB6B86710B5491...	Date Approved: 9/2/2016

I. POLICY STATEMENT

This policy governs the receipt, removal and movement of hardware, electronic devices and media that contain confidential or sensitive information, including EPHI, into and out of CEHS HCC, and the movement of the devices and media containing this information.

II. DEFINITIONS

See HIPAA Privacy Policy 100

Device – The unit that uses the media and provides a physical interface.

Media – Media is what holds the information, (e.g., disk, platen, CD, magnetic stripe).

NOTE: For devices that have removable media, such as CD/DVD players the distinction is easy. For other devices where the media is an integral part of the device, the distinction is not so easy because the media is not designed to be removed, (e.g. hard drive, thumb drive, etc.).

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the health care component (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

Media Disposal Standard

1. All Healthcare devices, systems and their associated electronic media containing EPHI must be disposed of securely and safety when no longer required. Questions concerning the destruction of EPHI should be directed to the CEHS Privacy and/or Security Officer(s). Proper disposal methods include, but are not limited to:
    a. Clearing - Using software or hardware products to overwrite media with non-sensitive data.
    b. Purging - Degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domain or,
    c. Destroying - Disintegration, pulverizing, melting, incinerating, shredding, etc.

2. If an outside service is utilized for the disposal of a device or media, the devices or media must be marked as containing confidential or sensitive information before it goes off site for disposal and a business associate agreement must exist with the disposal vendor.

Media Re-Use Standard

1. Media and devices that contains confidential or sensitive information, including EPHI, should not be re-used without proper destruction of the data by degaussing, or overwriting the entire media a least once with pseudorandom data.

Media Accountability Standard

1. All devices and media containing EPHI that is received by or removed from a sensitive area must be appropriately tracked and logged by the HCC management and system administrator. The following information should be logged:
    a. Workforce member's name.
    b. Device and media name.
    c. The information affected.
    d. The reason for the movement.
    e. Date and time of check out or transfer.
    f. Date and time of check-in or transfer.
2. If the device and/or media that contains confidential or sensitive information, including EPHI, is to be transferred to an off-site location, the data on the media should be encrypted and the encryption and decryption keys are to be protected with the same care as the data.
3. Media tracking mechanisms are to be implemented to track the accountability of media into and out of CEHS and HCC.
4. When a device or media containing confidential or sensitive information such as EPHI is released for off-site maintenance or storage, a legally binding contract for the management of the information (i.e., a Business Associate Agreement) must be in place to protect the confidentiality and integrity of the data.

Data Back-Up and Storage

1. All confidential or sensitive information, including EPHI, will be backed up on a daily basis to some form of media and stored in an appropriate setting.
2. Devices and media containing confidential or sensitive information, including EPHI, must be stored in a physically separate, environmentally appropriate location from where the computing device being backed up resides and that is secure and protected from being lost or stolen.
3. Back-ups must be in encrypted format.
4. Restore procedures must be tested regularly to verify that backups are valid and restorable.

Mobile Device Procedures

Additional safeguards and procedures are required for mobile devices storing confidential or sensitive information. These devices include smart phones, mobile messaging devices, Personal Digital Assistants (PDAs) and USB flash drives.

1. Only encrypted email is considered to be a safe delivery method for EPHI. If encrypted email is not available, CEHS business containing EPHI should be done using Box.
2. All mobile devices that will be used must be taken to the CEHS Security Officer to have appropriate safeguards installed.
3. CEHS designated Mobile Device Management program must be installed on any mobile device by the Security Officer.
4. All data transferred from the USU network and applications remain the property of USU and come under the Confidentiality agreement of the workforce member (regardless of whether the individual paid for the device personally or was reimbursed for the item).
5. Files or applications used to store USU system passwords, pass phrases, PINS, etc. must be encrypted or password protected themselves.
6. Confidential or sensitive electronic information may not be stored locally without encryption.
7. End users are expected to take reasonable steps to prevent the loss or theft of the device.
8. Loss or theft of the device must be reported to the CEHS Security and/or Privacy Officer(s) immediately.
9. In the event of loss or theft, remote kill software will be used to destroy all USU/CEHS data on a mobile device containing confidential or sensitive electronic information.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.310 (d)(1)

45 CFR §164.310(d)(2)(i), (ii), (iii), (iv)