POLICY INFORMATION

<table>
<thead>
<tr>
<th>Document # 4000</th>
<th>Title: Device and Media Controls</th>
<th>Original Effective Date: 9/2/2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguard:</td>
<td>Approved by: Dean Beth E. Foley</td>
<td>Date Reviewed: 09/15/2017 10/02/2019</td>
</tr>
</tbody>
</table>

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 Health Care Components (HCC), and the movement of the devices and media containing this information. It is the responsibility of any workforce member who uses or is required to maintain hardware, electronic devices or electronic media that contains ePHI to comply with policy.

II. DEFINITIONS

See HIPAA Privacy Policy 100

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 health care devices, systems and their associated electronic media containing ePHI must be disposed of securely and safely 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 for irreversibly destroying ePHI include, but are not limited to:
   a. Disk wiping - 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. Best practice will be to destroy the media.
   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. Prior to device or media re-use, all ePHI stored on the device or media must be securely removed. Removal may be accomplished by disk wiping or by utilizing a reliable data destruction utility to ensure the data is non-recoverable. Caution: a typical disk reformat is not sufficient to comply with this requirement.
2. If required, a backup copy of the stored ePHI can be made prior to re-use of the media or storage device if the ePHI is needed for future use or retention purposes. If a backup copy is created it must have access authorization and safeguards in place (such as password protection, duo authentication, etc.) to prevent unauthorized access to the ePHI.
3. A written record of any reused or redistributed storage device or media must be created.

**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 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 Business Associate Agreement must be in place.

**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 an appropriate secure location.
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 could include but are not limited to 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 and CEHS IT department to have appropriate safeguards installed.
3. CEHS designated Mobile Device Management program must be installed on any mobile device.
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.
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 Compliance Officer immediately.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.310 (d)(1)
45 CFR §164.310(d)(2)(i), (ii), (iii), (iv)