Oklahoma State University

Title: Electronic Media Disposal & Re-use	**Policy #: SEC-11.01**
Category: HIPAA Compliance	**Authority: 45 CFR §** **HIPAA SECTION: 164.310(d)(2)(i)**
Standard: Device & Media Controls	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Page 1 of 3**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

The purpose of this policy is to address the appropriate protection of sensitive electronic information (SEI) when it is stored, transferred or accessed on portable devices such as: Laptops / PDAs / Smart Phones (devices with operating systems) or removable media such as: USB Flash drives / Memory cards / Floppy Disks / CDs / DVDs. This policy is not intended to address non-classified data.

This policy covers all OSU-owned, leased, or managed portable devices or removable media. At the discretion of the organization, it also may apply to any third-party (e.g., staff member or contractor) owned or managed devices or media as a pre-condition for being granted authorization to OSU-managed SEI..

POLICY:

OSU will implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. *§164.310(d)(2)(i)*

OSU will implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. *§164.310(d)(2)(ii)*

Measures must be followed on hardware and software installations as well as user conduct to ensure that the integrity and security of the data is not compromised. All electronic media that is to be decommissioned or repurposed must have all PHI removed so that no private or confidential information is retrievable from the media according to Department of Defense decommissioning and NIST standards. Electronic media includes, but is not limited to, tapes, hard drives, solid state storage units, compact disks (CDs), and thumb drives. If the media cannot be sanitized, such as with CDs, the media must be physically destroyed. The purpose of this policy is to outline the precautions to protect data that is stored on all electronic media.

The workforce shall take all reasonable and prudent measures to ensure the safety and confidentially of all Sensitive Electronic Information that is downloaded to any removable media or portable device. e.g. PDA, laptop, etc. Reasonable measures include but are not limited to: storing large files and databases only on network shares, password protecting sensitive files or using an approved encryption method.

The workforce shall take all reasonable and prudent measures to physically secure all removable media or to portable devices. Users shall not open or attempt to open the encasement of any removable media or portable devices nor otherwise circumvent any lock system that secures the device or its components. User should take reasonable measure to secure device at all time and report any lost or stolen removable media or portable devices immediately.

Oklahoma State University

Title: Electronic Media Disposal & Re-use	**Policy #: SEC-11.01**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.310(d)(2)(i)**
Standard: Device & Media Controls	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Page 2 of 3**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PROCEDURE:

Hardware

Desktops and laptops are to be configured by Information Technology personnel before they are installed. Configuration is defined by the Information Technology Department. Users must call the Help Desk for assistance from Information Technology personnel in disconnecting and reconnecting the desktop in the event of an office move. The Inventory Transfer form must be complete before the move to ensure that moveable equipment inventory (MEI) will contain the correct location of the device.

All OSU campuses are responsible for tracking inventory.

When any computing device (desktop, laptop, printer, etc.) has lived out its useful life or is being repurposed, the user must complete a Fixed Asset Disposal Request form or a Fixed Asset Transfer Request form whichever is applicable and send the completed form to the Purchasing Department. Purchasing department personnel will arrange with the Facilities Department to retrieve the equipment. All servers, desktops and laptops are delivered to I.T. for decommissioning of the hard drive. Appropriate computer personnel will eliminate all data from the hard drive to the DOD & NIST standards before the hardware is moved, salvaged, or auctioned. Hard drives that cannot be decommissioned are physically removed and destroyed. A Computer Decommissioning/Sanitation Form will be completed for each laptop and desktop hard drive that is decommissioned. A copy of the Decommissioning/Sanitation Form will be attached to the desktop or laptop. A copy of the Decommissioning/Sanitation Form and the Inventory Disposal Form are made and kept in the I.T. department records. The originals of the Inventory Disposal Form and the Decommissioning/Sanitation Form are sent to the Purchasing Department. A log is maintained of all sanitizing actions identifying the media owner, media type, date of completion, and the name of the staff member or members who perform the sanitization. If IT receives a Hard Drive from a vendor for destruction, IT will make a best effort to appropriately complete the Computer Decommissioning/Sanitation Form.

Software

Information Technology and associated vendors will be the only individuals approved to install operating or application software on the network. Users must call the Help Desk to request the installation of software for their desktop or laptop. Proof of licensing will be required before the software can be installed. If a user requires assistance with removing desktop software, they should call the Help Desk for assistance. Any permanent backups required of the desktop/laptop will be the responsibility of the user. If a software package that is installed on the network becomes obsolete the removal request should be made through the Help Desk. Information Technology will ensure that no one is referencing the software and make the necessary permanent backups before removing the software.

Oklahoma State University

Title: Electronic Media Disposal & Re-use	**Policy #: SEC-11.01**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.310(d)(2)(i)**
Standard: Device & Media Controls	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Page 3 of 3**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

Media

The media used in creating the official backup will be housed in locked computer rooms on the appropriate campuses. Information Technology personnel will be handling the transport of this media to its off-site storage location. Refer to Contingency Planning Backup for details.

Media that is obsolete, has been requested to be destroyed, and that cannot be sanitized as described above under the hardware procedures should be sent to I.T. for destruction. A log is maintained of all destruction actions identifying the media owner, media type, date of completion, and the name of the staff member or members who perform the destruction.

Users must protect their data and files by preventing unauthorized access. Users must protect their storage media by not leaving their storage media lying around and locking up their storage media. Users must not make copies of data files with identifiable data or data that would allow individual identities to be deduced unless specifically authorized to do so.

Additional References

Setting Up Users' PCs
Fixed Asset Transfer Request
Fixed Asset Disposal Request
Contingency Planning Backup