UNM HEALTH SCIENCES CENTER

Applies To: **All HSC Workforce Members**
Responsible Department: **Information Technology**
Revised: **New**

Title: **HSC Computer and Electronic Device Inventory**	**Standards and Guidelines**

DESCRIPTION/SCOPE

This standard establishes common practices and guidelines for the inventory of UNM Health Science Center (HSC) computer equipment. This standard also establishes a common standard for documenting attributes that describe each computer item. These standards are aligned to the yearly physical inventory requirements with the addition of certain computer network attributes that can be used to link an automated network inventory of active devices to this computer inventory. By linking the physical inventory, the computer inventory, and the automated network inventory, devices can be managed and maintained according to their device classification and associated procedures for addressing configuration, patch management and accountability.

UNM Health Sciences Center policies apply to all health care components of UNM that are under the jurisdiction of the HSC as designated in UNM Board of Regents Policy 3.4 Subject: Health Sciences Center and Services and UNM Board of Regents Policy 3.7 Subject: Institutional Compliance Program.

REFERENCES

See HSC Policies, including but not limited to: HSC-300 ePHI Security Compliance, HSC-260 Device and Media Control, HSC-270 Information Systems Activity Review and UNM Policy 7710 Property Management and Control.

DEFINITIONS

Computer: UNM Policy defines a computer as, “items such as laptops, desktop workstations, and tablets”. For inventory purposes the HSC defines computers as including the following devices:

- A Desktop or workstation (may include a keyboard, mouse and monitor)
- A Server (including tower, rack, blade, or similar configurations)
- A Laptop or Notebook Computer (integrated standard keyboard)
- A Tablet computer (touch screen computer)
- Other (anything that is capable of connecting to the network that has been assigned a property tag number)

Electronic Devices:

- A Networked Device with a Property Tag: Electronic devices capable of connecting to the HSC network that have been assigned a property tag number.
- A Networked Device without a Property Tag (e.g., printers, VOIP phones, etc.): These devices may be included on the component’s inventory at the discretion of the component based on a risk assessment. If not included on the inventory the devices may be managed through other practices and procedures established through risk assessments. Electronic devices are subject to one or more of the following: network access controls, network scans (network fingerprinting or vulnerability scans), and network restrictions based on the device

classification.

- Digital storage media such as backup tapes, DVDs, CD, USB storage devices, etc. that contain Confidential information (ePHI) of significant value/risk shall be included on the inventory or managed according to other appropriate standards.

Computer Inventory Attribute Guidelines: A spreadsheet, database or other structured electronic data management tool that includes the following information.
Required Attributes:

- Inventory identification number (property tag or other unique number)
- Description of item (desktop, server, laptop/notebook, tablet, printer, other)
- Computer Name / Host Name (if configured)
- Network MAC Address (if capable of network access)
- Owning Department name/number
- Location type (public, access controlled, data center, mobile, secured room, other)
- Status (A-active, I-Inactive, T-transferred, S-salvaged)
- Authorized to store ePHI files (Y/N)

Optional Attributes:

- Manufacturer, model number, and serial number
- Purchase reference number (if available)
- Building number
- Room (if available)
- Original Cost or Estimated Value (<$1K, $1K to $5K, >$5K) (if available)
- Other attributes as deemed necessary for IT operations

STANDARD

1. **Asset Management**

The tangible results of a linked and consolidated, risk-based, whole life cycle asset management approach are:

- Alignment of processes, resources and functional contributions for improved planning (instead of departmental silos with competing short-term priorities)
- Creating a transparent audit trail for what is done, when and why
- Better understanding and usage of data and information to provide informed and consistent decisions
- Consistent, prioritized and auditable risk management
- Alignment and coordination of existing initiatives
- Greater engagement of the workforce, including leadership, communications and cross-disciplinary teamwork

1.1. **Data and System Classification**

HSC Information Assets, computers and electronic devices defined above are to be classified based on the impact to business operations as well as risk to confidentiality, and include but are not limited to the following classifications:

A. Data Classification

1) Primary Source ePHI (involved in direct patient care)
2) Secondary Source ePHI (involved in operations, billing, and research)

B. Computer and System Classifications
   1) Critical ePHI System (devices used for collecting, storing, processing or transmitting Primary Source ePHI)
   2) Basic ePHI System with Encryption (devices approved for storing Secondary Source ePHI for operations, billing and/or research – encryption required)
   3) Basic ePHI System (devices only used for accessing ePHI)

HSC computer and electronic devices classified according to this standard must be included in the computer inventory. Additionally, if the device stores ePHI the inventory must reflect that the device is authorized for such use.

PROCEDURES

1. The HSC Unit Security Liaison will work with the unit's facilities and inventory management staff to provide a complete inventory of the unit's computers as defined by this standard. The inventory will include and be structured according the computer inventory definitions and attribute guidelines defined above.

2. The inventory may be gathered from existing inventory data but must be structured as defined above or as indicated in sample spreadsheets and databases that are available on request.

3. Each HSC Unit Security Liaison will have 60 days from the date of the yearly notice to provide a current and accurate report of computer inventory. An extension in the due date can be granted if approved by the IT Security Council. Only devices that will be in active use by the unit during the current physical inventory reporting period should be reported. Status change for inventory items previously reported that have been transferred or salvaged should be noted in the report.

HSC Components

The following units and individuals comprise the Unit Security Liaison program.

1. UNMH	David Grisham
2. UNMMG	Michael Basile
3. SOM (all programs/centers unless noted below)	Jeanne Marquardt
Programs or Centers under SOM	
4. OMI	Amy Boule
5. CDD	Dan Wenz
6. UNMCC	Laura Olszewski
7. CON	Alex Flores
8. COP	Irmin Wehmeier
9. HSLIC	Gayle Shipp
10. HSC Administration	Paige Briggs

11. HSC Office of Research	Cathy Penick
12. Sandoval Region Medical Center	Randy Ferguson
13. HSC Office of Community Health	Adrian Rodriguez

Documentation Standards and Guidelines

1. Inventory records kept for Computers, Electronic Devices or Storage Media containing ePHI shall indicate if the device or media was transferred or destroyed. All sensitive data is to be wiped before items are transferred or destroyed according to appropriate disposal procedures.
2. Computer Inventory Reports of items defined in this Standard and that may contain ePHI are to be retained for at least six years.

Exceptions

Any exception to the HSC Computer Inventory Standards and Guidelines must be approved by the HSC Information Security Officer who will maintain a record of all systems that have been granted such an exception.

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Barney Metzner, HSC ISO, HIPAA Security Officer		
Consultant(s)	HSC Task Force on IT Security Standards HSC Information Security Officer		
Committee(s)	HSC IT Security Council HSC KMIT OPS Committee		Y
Official Approver	Holly Shipp Buchanan, EdD, HSC CIO		Y
Official Signature		1/9/2013	
Official Approver	Glen Jornigan, UNMH IT Administrator		
Official Signature		1/9/2013	
Effective Date		1/9/2013	
Origination Date		11/2012	
Issue Date	Clinical Operations Policy Coordinator	1/28/2013	ar

INITIAL APPROVAL BY HSC IT SECURITY COUNCIL: 11/15/2012