UC Riverside, School of Medicine Policies and Procedures
Policy Title: IT Asset Management
Policy Number: 950-02-205

Responsible Officer:	Information Security Officer
Responsible Office:	UC Riverside School of Medicine (UCR SOM) Compliance Department
Origination Date:	03/23/2017
Date of Revision:	Not Applicable
Scope:	• All UCR SOM information, in an electronic format, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it • All Technology Infrastructure owned and/or administered by UCR SOM • All UCR SOM divisions, including those of UCR SOM subsidiaries, if any • All UCR SOM workforce members, including employees, interns, contractors, consultants, and vendors doing business with UCR SOM including any individuals affiliated with third parties that access UCR SOM systems

I. Policy Summary

The purpose of this policy is to define UCR SOM's requirements regarding the management of IT assets, or other technology asset that may store, process or transmit electronic Protected Health Information (ePHI).

II. Definitions

IT Assets – Any electronic device that either: a. connects to the computing network, or b. stores, processes or transmits electronic data.

For other definitions, please refer to Standard Definitions Guide.

III. Policy Text

UCR SOM manages the acquisition, distribution, use, and destruction of all IT assets purchased by a workforce member of UCR SOM for business use.

Acquisition of Assets

UCR SOM IT assets shall be acquired following approved OIT procedures. At a minimum, all acquisition of technology will meet the following requirements:

A. Business Case

A document summarizing the business justifications and requirements for a particular technology.

B. Security Evaluation

A completed, reviewed, and approved copy of the System Risk Assessment (SRA) form must be completed prior to implementation of the new technology.

C. Assigned Owner

A business owner responsible for the maintenance, security, and decommissioning must be assigned to every acquired technology.

D. Asset Inventory

The new technology will be entered into the approved OIT asset management system. If the technology stores, processes, or transmits ePHI, this will be noted in the asset inventory system.

IV. Responsibilities

A. Office of Information Technology (OIT)

1. Make initial entry in asset management system including location, asset purpose, ePHI access, asset tag number, asset name (if applicable), and any other pertinent information regarding the asset.
2. If the asset is a physical device, as opposed to a software license, create or acquire the necessary asset tag on the asset.
3. If the asset needs to be shipped to another facility, OIT will arrange shipping and verify the new location.
4. Tracking the location of all assets in the asset management system.
5. Separation of writable media from the asset upon end of life.
6. Proper destruction, sale, or reuse of the asset. (In the case of non-OIT owned assets such as medical devices, OIT will be responsible for verifying the process).
7. Performing an annual inventory of all assets in the asset management system.
8. Notifying the Information Security Officer of new asset for risk assessment.

B. Information Security/Compliance Office

1. Perform security risk assessment on any new technology and review annually.
2. Test the asset management process.
3. Review asset management reports, including destruction reports, location verification, and proper identification of assets.

V. Procedures (Not Applicable)

VI. Forms and Attachments (Not Applicable)

VII. Related Information (Not Applicable)

VIII. Revision History - New Policy

Approval(s):

COMPLIANCE COMMITTEE (07/25/2017)