BSD & UCM Cyber Security Policy Summary
Policy Name: Media Protection Policy
Date: September 14, 2015

Purpose

The Media Protection Policy provides procedures on how to properly store, move and dispose of information stored on Electronic Media (e.g. thumb drives, external hard drives, hard drives, etc) to minimize the risks of improper disclosure, access or theft of information with significant purpose or meaning (e.g. Patient records, Social Security Numbers, Credit Cards).

Policy Summary

Definitions

- **Protected Information** - Information that needs to be protected, as mandated by laws or regulations (e.g. Patient records, Social Security Numbers etc..).
- **Electronic Media** - Storage material on which data is or may be recorded electronically such as hard disk drive or digital memory card (e.g. USB flash drives, CDs/DVDs, external hard drives and internal hard drives).
- **Mobile Device** - A portable, wireless computing device that is small enough to be used while held in the hand, such as smartphones, tablets and laptops.
- **Covered Individuals** - Employees and students in UCMC and BSD (e.g. Administrators, Faculty, Staff and Users) including third parties with access to the Organizations' Information Systems.
- **Information System Owners** - Employees of the Organization, Director level or above who have the ultimate responsibility over a particular Information System.

General Summary

- Protected Information must be encrypted when stored on desktops, laptops, phones and tablets.
- Newly purchased Mobile Devices including thumb drives, and external hard drives must be encrypted regardless of the information store when device is used for business purposes.
- Information System Owners will ensure that Protected Information is properly sanitized prior to disposal, release, or reuse.
- Physical access to Electronic Media must be restricted to the appropriate personnel or role-holders.
- Departmental and Unit Leaders will ensure that staff under their supervision properly handles the protection, release and disposal of information on Electronic Media.
- A summary of the responsibilities outlined in the policy are provided in the table below.

Roles Responsibilities	Administrators Faculty, Staff and Users	Information System Owners and IT Staff	Departmental and Unit Leaders
Encrypt mobile devices and electronic media (e.g. Laptops, phones, thump drives etc.)	✓	✓	
Properly sanitize electronic media with Protected Information prior to disposal, release or reuse.		✓	
Restrict access to Electronic Media to the appropriate personnel or role-holders.	✓	✓	
Ensure staff properly handles protection, release and disposal of information on Electronic Media.			✓