BSD & UCM Cyber Security Policy Summary
Policy Name: Personal Computing Device Policy
Date: September 14, 2015

Purpose

The **Personal Computing Device** defines the responsibilities of our faculty, employees, students and staff as it relates to securing their own personally owned computer equipment when it is used for University of Chicago Medicine and BSD purposes. Personal computing equipment commonly involves items like iPhones, iPads, Android devices, tablets, and laptops. It also includes items like removable storage devices (flash drives) and external hard drives. The target audience of this policy is the Organizations' users.

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..).
- **Device** – Any desktop or laptop computer (e.g., Windows, Mac, Linux/Unix) or portable device (e.g. smart phone, tablet etc.) used for business purposes.
- **Covered Individuals** - Employees and students at UCMC and BSD (e.g. Administrators, Faculty, Staff and Users) including third parties with access to the Organizations' Information Systems.
- **Departmental and Unit Leaders** - Department Chairs, Section Chiefs, Executive Directors, Directors, Managers, Supervisors, etc.
- **Information Owner** - Employees of the Organization who are Director level, faculty, or above, responsible for classifying Information and ensuring access to the information is appropriate.

General Summary

- Employees have a right to use their personal devices for business purposes as long as they agree to secure the devices in accordance with policy, and follow specific procedures.
- The Security Officers' have a right to enforce the security on these devices, when the Covered Individual elects to use the device for business purposes. Examples of enforcing security include a) enforcing a passcode on the device, b) enforcing encryption be enabled before accessing email and c) enforce the device will be wiped if a passcode is entered incorrectly more than 10 times.
- The policy sets the expectations around what the employee will do with regard to data and licenses used on the personal devices, should the employee no longer be affiliated with the BSD or UCM.
- 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
Ensure devices have proper security controls	✓		
Enforce security measures on personal devices	✓	✓	
Ensure Covered Individuals are abiding by policy			✓