# Mobile Computing Device Standard

## Scope

As mobile devices further incorporate features traditionally found in a personal computer, their smaller size and affordability make these devices a valuable tool in a wide variety of applications. However, these devices are also subject to increased risk of loss, theft, and unauthorized use.

These standards apply to all University of Rochester and University of Rochester Medical Center and Affiliates faculty, physicians, staff, students, volunteers, vendors, contractors, workforce members and any others who utilize a mobile device to access or store the University of Rochester's or URMC & Affiliates nonpublic information, including email and other electronic data, regardless of ownership of the device.

## Purpose

These standards establish base configurations and management guidelines for mobile computing devices (e.g., cellular or smart phones, laptops, tablets, etc.) owned and/or operated by the University of Rochester or its workforce. As there are a wide variety of mobile device operating systems, software, and system configurations used across the University, this document is NOT intended to be a definitive and comprehensive guide to device security.

Compliance with these standards does not exempt a device from meeting federal, state, or local laws and regulations. For example, if the device is collecting or storing credit card data, then the application and server must comply with all Payment Card Industry (PCI) standards.

Effective implementation of these standards will minimize the likelihood of unauthorized access to University computing resources and legally restricted and/or confidential information. All security events (e.g., loss of, or unauthorized access to device) must be reported to the appropriate Chief Information Security or Privacy Officer as soon as they are discovered, in order to ensure compliance with legal obligations.

## Requirements

- **Physical Protection:** Individuals must keep mobile devices with them at all times or store them in a secure location when not in use.
- **Password Protection:** Access to the mobile device must be protected by the use of a password.
- **Encryption:** University data classified as Legally Restricted Information must not be stored on a storage card or the device (including within cached email) without proper encryption, password protection and inactivity timeout.
- **Inactivity Time-out Protection:** Inactivity timeout must be set. The recommended inactivity timeout is 15 minutes but must not exceed 60 minutes.
- **Proper Disposal:** Any residual settings, data, and applications on the mobile device must be removed or wiped prior to disposal or transfer to another user. All attached storage cards that contain Legally Restricted Information must be destroyed or wiped so no data recovery is possible.
- **Lost or Stolen Device:** If a mobile device containing University of Rochester information is lost or stolen, report the loss immediately to University of Rochester Security, the University or Medical Center Chief Information Security Officer, and a Privacy Officer (if it was used to access or store Medical Center information). These individuals will determine whether there is any requirement to report the security incident to state or federal agencies or others. In addition, the incident must also be reported immediately to the appropriate information technology Help Desk to determine if the device can be wiped remotely.
- **Secure Connectivity:** Any Legally Restricted information transmitted to or from the mobile device (e.g., wireless or the Internet) should be encrypted. Communication protocols such as SMS (Text Messaging) are not considered secure and in some cases, like for Protected Health Information (PHI), may result in a breach of confidentiality.
- **Only Use Approved Cloud Storage:** Many applications and operating systems on mobile devices now encourage or make readily available the ability for users to utilize cloud storage. It is important to consider that the use of cloud

storage may violate certain Privacy and/or Security regulations and laws covering where certain types of data are allowed to be stored. For example, electronic PHI is only allowed to be stored with 3rd parties who have completed appropriate contracting with the University of Rochester or URMC & Affiliates. Any data stored on unapproved storage would result in a breach of confidentiality. Please contact the Help Desks to configure an account on approved cloud storage.

### Additional Recommendations for Mobile Devices

- **Invalid Password Attempts:** The device should be set to wipe after 10 invalid password attempts.
- **Disabling Unused Services:** Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.
- **Remote Wipe Capability:** The mobile device should support the ability to remotely reset the device, including the deletion of all locally stored data.

### Need Help?

For additional information or assistance with configuring your device:

University IT Help: (585) 275-2000 or univithelp@rochester.edu

Medical Center IT Help: (585) 275-3200 or helpdesk_ISD@URMC.rochester.edu

For any questions related to this document or the requirements, please contact the University of Rochester Information Security Office (InfoSec@Rochester.edu)

### Definitions

Mobile device: includes any device that is both portable and capable of collecting, storing, transmitting, or processing electronic data or images. Examples include, but are not limited to, laptops or tablet PCs such as iPads and netbooks, personal digital assistants (PDAs), and "smart" phones such as Blackberry, iPhones, Android devices, etc. This definition also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device.

## Appendix 1: Revision History

| Modification(s) Made | Modified by: | Date of Modification | Reviewer | Review Date |
|---|---|---|---|---|
| Document Adopted | University IT | 6/6/2011 | University IT | 6/6/2011 |
| Document Updated | Information Security Office | 2/27/2018 | Privacy Security Executive Committee | 3/1/2018 |

## Appendix 2: Contact Information

Please address any questions or concerns with any procedures set forth within this document to the University of Rochester Information Security Office <InfoSec@Rochester.edu>.

## Appendix 3: Related Policies and Procedures

University IT Information Security Policy
Data Security Classifications Policy
0SEC01 Access Control
0SEC06 Compliance

0SEC07 Asset Management
0SEC08 Physical and Environmental Security
0SEC09 Communications and Operations Management
0SEC10 Information Systems Acquisition, Development and Maintenance
0SEC11 Information Security Incident Management