

Information Technology Standards

Mobile Device Security

IT Standard Issued: 9/16/2009

Supersedes: New Standard

Responsible Executive: HSC CIO

Responsible Office: HSC IT

Contact: For questions about this standard, please contact The HSC Security Officer. For assistance in complying with this standard, please call user support at HSLIC – 272-1694 or UNMH at 272-DATA.

Summary of Standard: 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, breakage, theft and unauthorized use.

Glossary:

HSC Mobile device: includes any HSC owned 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, personal digital assistants (PDAs), and “smart” phones such as Blackberries. 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.

This standard does not apply to device covered by other standards, such as security badges with magnetic or embedded storage technologies or any mobile medical device not intended as a personal computing, communication or storage device.

Personal mobile device: includes any mobile device that is **not** owned or issued by the University of New Mexico Health Sciences Center.

Sensitive information: includes, but is not limited to,

- **Personal identity information (PII):** includes Social Security Numbers, credit card numbers, bank and credit union account numbers, health insurance plan identification numbers, drivers license numbers, dates of birth, and other similar information associated with an individual student or employee that, misused, might enable assumption of that individual's identity ("identity theft") to compromise that person's personal or financial security.
- **Protected health information (PHI):** includes health information that is associated with at least one of eighteen identifiers that make the information “individually identifiable.” The eighteen identifiers include name, address, SSN, date of birth, date of health care, and other elements listed in the HIPAA regulations. Health information about groups of people (population data, mean and median data, aggregate data, etc.) that cannot be related to individuals is not PHI.
- **Student educational record information:** includes records that are based on student status and maintained by the University or a party acting for the University. Access to student records is governed by the UNM Student Records Policy and the Family Educational Rights and Privacy Act (FERPA). Sole possession records, medical or psychological records, alumni records, employment records, and law enforcement records are not considered student educational records and not subject to FERPA.

Who is Affected by this Standard: All HSC faculty, staff, and students; employees of the University Medical Group UMG; .as well as vendors, contractors or any others who utilize a HSC mobile device to access the HSC network or store HSC information. This policy applies to everyone at all campuses and sites of the HSC. There are no exemptions.

Resources: All electronic HSC mobile devices that are used to access the University of New Mexico Health Science Center's network or to store UNM HSC information.

Why We Have this Standard: The purpose of this standard is to provide guidelines for the appropriate use and configuration of HSC mobile devices as necessary to protect the restricted HSC network and/or information from unauthorized access or disclosure.

Responsibilities:

Standards:

I. General Guidelines for the Use of HSC Mobile Devices

- Personal mobile devices that are used to access the UNM HSC network must conform to the security requirements outlined in the HSC's Information Technology Standards for Users
- Recovery software. All portable computers (laptops and tablets) owned by the University or the HSC Research Institutes must have tracking data or software installed to enable their identification and retrieval in the event of loss or theft.
- Physical protection. Mobile devices owned or issued by the University must not be left unattended in a public space and, where possible, must be physically locked away or secured
- Device identification. All laptops, tablets, PDAs, Blackberries, smart phones and portable hard drives owned or issued by the University must be permanently marked as "Property of the University of New Mexico or UNM Hospitals" and indicate a method of return if the device is lost.
- Virus protection. Any HSC mobile device that is capable of using antivirus software must have the software installed and configured to maintain updated virus software and signatures. Contact Support/Help Desk (2-DATA,2-1694) for information on approved antivirus software.
- Security Updates. A procedure must be established and implemented to ensure that all security patches and updates relevant to the device or installed applications are promptly applied in compliance with the HSC's Standards.
- Disable unused services. Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.
- Storage of passwords. The storage of user IDs and passwords which allow access to the HSC network or its systems is prohibited on all mobile devices, unless done in accordance with approved HSC Standards.
- Termination of University relationship. All University-owned mobile devices must be returned to the appropriate HSC department immediately upon termination of the assigned user's relationship with the department or

University. In addition, any software applications purchased by the University and installed on personal mobile devices must be removed immediately by the user.

- Report any suspected misuse or theft of a mobile device immediately to Information Security and the campus police.

II. Additional Requirements for HSC Mobile Devices Used to Access or Store Sensitive Information

The following represent “best practices” for anyone utilizing a mobile device; however, HSC mobile devices used to access or store sensitive information must meet the following requirements.

- Access and use sensitive information appropriately. Sensitive information must not be stored on mobile devices without prior approval from your department Director or Chair. For more information on identifying and handling sensitive information, refer to... (Data Classification Standard, locate at <http://cio.unm.edu/standards/index.html>)
- Use of personal devices is restricted. Official records may only be stored on or accessed directly by mobile devices that are owned, issued or approved for use in writing by UNM or UNMH.
- Use of personal USB drives (also known as "thumb drives") or such devices without proper encryption and password protection for the storage of sensitive information is prohibited.
- Device registration and certification. Any mobile device used to access or store sensitive information must be registered with and certified by Information Technology Security prior to its use. Contact the Information Security staff for information about mobile device registration and certification.
- Physical protection. Users must make every reasonable effort to physically secure mobile devices. Mobile devices used to access or store sensitive information must not be left unattended in public or other unsecured areas and, where possible, must be physically locked away or secured. In addition, any portable media (for example, portable hard drives, CD-R or DVD-R disks used for backup of systems containing sensitive information must be stored securely in locked drawers, cabinets or other secure enclosures.
- Exclusivity of use. Any mobile device that has been registered and approved to store sensitive information must not be shared with any other person without prior written approval from Information Security.
- Password protection. Access to the mobile device must be protected by the use of a password that meets the requirements outlined in the UNM password standard.
- Use of encryption. All mobile devices containing sensitive information must consistently encrypt all files using an encryption method that has been approved by Information Security. Contact the Information Security staff for information on approved encryption solutions.
- Secure connectivity. Any sensitive information transmitted to or from the mobile device (e.g., wireless or the Internet) must be encrypted.
- Synchronization. Mobile devices containing sensitive information must only synchronize data with sync stations, workstations or other devices that also have been approved for the storage of the sensitive information.

- Protection of information. Reasonable care must be taken when using mobile computing facilities in public places, meeting rooms or other unprotected areas outside of the HSC's premises to avoid the unauthorized access to or disclosure of the information stored on or accessed by the device.
- Termination of University or department relationship. Sensitive information must be removed from the device immediately upon termination of the assigned user's relationship with the University.
- Dispose of the device properly. Mobile devices and other electronic equipment that contain, are used to access sensitive information, or have been used to access sensitive information in the past must be disposed of as outlined in the HSC Policy titled "7.4 - Disposal - ePHI "
- Backup. Any single instance, critical data, stored on a HSC mobile device must be transferred to the official electronic medical record system for backup.

Exceptions

Requests for exceptions to this Policy may be granted only under special circumstances. Any requests must be submitted in writing to the Information Security Officer for approval.

Exceptions will be permitted only on receipt of written approval from Information Security. Information Security will retain documentation of currently permitted exceptions and will review them on an annual basis.

Enforcement

Suspected or known violations of this policy will be reported to the appropriate University officials, and may result in:

- Loss of individual computing privileges.
- Accountability for conduct under any applicable University or campus policies, procedures, or collective bargaining agreements, including disciplinary action.
- Disconnection of non-compliant systems from the UNM/HSC network

Suspected or known violations of University regulations and/or State and Federal law will be processed by the appropriate University authorities and/or law enforcement agencies.

Website Address for this Standard: <http://hsc.unm.edu/library/kmit/policies.shtml>

Related Documents:

HSC: Password Management ePHI, UNMH: IT Security- Password Management, Controls and Standards, HSC: Encryption ePHI, HSC: Workstation Use and Security ePHI, HSC: Disposal ePHI, UNMH: IT Security-ePHI Information Disposal

Contact information

For information on this policy, please contact:

**Information Security
Officer**

Barney Metzner
HSC Security Office
MSC09-5100
272-1696

HSC CIO

Dr. Holly Buchanan
HSC Chief Information
Officer
272-2548

UNMH CIO

Ron Margolis
Chief Information Officer
272-2168

Public Safety Officer

UNM Campus police
2500 Campus Blvd. NE, Hokona Hall
Albuquerque, NM 87124
505) 277-2241

To report suspected non-compliance activities to a corporate compliance officer:

UNM Hospitals 272-8761
University Physicians Associates 272-6036
SOM Office of Research 272-1887
HSC Compliance Hotline 1-888-899-6092 (anonymous)
HSC Legal Department 272-2463
UNMH Security Dispatch 272-2160