



University of Connecticut Health Center

POLICY NUMBER 2008-03

May 27, 2008

POLICY: MOBILE COMPUTING DEVICE (MCD) SECURITY

PURPOSE:

The University of Connecticut Health Center (UCHC) has established this policy for the secure implementation and deployment of mobile computing and storage devices within UCHC to support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements (e.g. HIPAA, NIH, HHS.)

SCOPE:

This policy applies to:

- Employees (including faculty and staff)
- Volunteers
- Residents
- Students
- Temporary staff
- Agency and contracted staff
- Credentialed staff
- Members of the Board of Directors

This policy covers portable or mobile computing and telecommunications devices (referred to as MCD's) that can execute programs or store data. Because all MCD equipment used at the Health Center is institutional property, regardless of funding source, this definition includes all UCHC laptop computers, PDAs, BlackBerry® devices, and USB storage devices.

DEFINITIONS:

Confidential or restricted data

Includes, but is not limited to, personally-identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual. Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals. This data may include, but is not limited to:

- Student information
- Medical/Dental/Behavioral Health-related patient information (ePHI)
- Other sensitive Health Center information not in the public domain
- Financial information about the Health Center (budgets, strategic revenue plans, accounts receivable/payable details)
- Employee HR and financial information
- Any information about employees, students, patients, Board Members, etc. which includes Social Security numbers
- IDs and/or Passwords for access to Health Center computing resources
- Research data requiring protections (clinical trials, patient survey responses, etc.) as required by the NIH

POLICY STATEMENTS:

Permissible Use

UCHC confidential or restricted data is not authorized to be stored on a UCHC or non-UCHC MCD unless the criteria below are met:

1. The device stores only the minimum data necessary to perform the function necessitating storage on the device
2. Information is stored only for the time needed to perform the function
3. The device is encrypted using methods authorized by the UCHC IT Department
4. Data is protected from any and all forms of unauthorized access and disclosure

IT Responsibilities

1. The UCHC IT Department will provide Mobile Computing Device users with approved and properly updated software-based security mechanisms which may include anti-virus, anti-spyware, device locating, encryption, firewalls, and intrusion detection.
2. The UCHC IT Department will work with the Security Breach Team to establish, document, and maintain reporting, mitigation and remediation procedures for lost or stolen mobile devices containing UCHC data and for UCHC data that is compromised through accidental or non-authorized access or disclosure.

Mobile Computer Device User Responsibilities

1. Users may not bypass or disable security mechanisms under any circumstances.
2. Users in the possession of UCHC-owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas must not leave these devices unattended at any time, and must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft.

3. Unauthorized physical access, tampering, loss or theft of the device must immediately be reported to the UCHC IT Help Desk in order to initiate effective and timely response and remediation.
4. Basic Science users who do not store confidential or restricted data may optionally use the device encryption software provided and supported by the UCHC IT Department.

Governance

1. Failure to adhere to this security policy and associated procedures may result in sanctions as per applicable UCHC policy.

Sandra Armstrong (signed)

June 16, 2008

Chief Information Officer

Date

Peter Deckers, M.D. (signed)

June 18, 2008

Executive Vice President for Health Affairs

Date

**Replaces Policy #2003-32 Originally issued 4/14/03
Updated: May 27, 2008**