UCONN HEALTH

POLICY NUMBER 2008-03
February 17, 2015

POLICY: MOBILE COMPUTING DEVICE (MCD) SECURITY

PURPOSE:
UConn Health has established this policy for the secure connection and deployment of mobile computing and storage devices within UConn Health to support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements (e.g. HIPAA, local, state and federal laws, 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 mobile telecommunication and mobile computing devices which can execute programs or store data. This policy defines the requirements that must be followed when connecting either institutionally or personally-owned Mobile Computing Devices (MCDs) to UConn Health's systems or networks. All MCD equipment procured by and/or funded by UConn Health is institutional property, regardless of the source of funds from which they were purchased.

DEFINITIONS:
Mobile Computing Device (MCD): Includes laptop and tablet computers, smartphones, and external storage devices. All forms of data are covered by this policy, including but not limited to: any systems used to capture electronic data, as well as any media used for creating, obtaining or capturing data.

Confidential 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 and/or the institution. Such harm might include but is not limited to:

- actions resulting in significant, severe or catastrophic harm to individuals;
- causing a significant or severe degradation in mission capability;
- causing significant or major damage to organizational assets;
- actions resulting in significant or major financial loss; or
- actions resulting in sanctions against UConn Health by a governmental or regulatory body.

Examples of such data may include, but are not limited to:

- Certain student information
- Medical/Dental/Behavioral Health-related patient information (PHI)
- Other sensitive UConn Health information not in the public domain
- Financial information (budgets, strategic revenue plans, accounts receivable/payable details) **NOTE: Credit card numbers are not to be collected, transmitted, or stored on UConn Health's computing devices and networks under any circumstances.** Posting credit card information to a vendor website for authorized purposes using UConn Health's computing devices is allowed. Sending credit card information via email for any reason is not allowed. For any questions please contact the Information Security Office
- Employee human resources and financial information
- Any information about employees, students, patients, Board Members, etc. that includes Social Security numbers
- IDs and/or Passwords for access to UConn Health computing resources
- Research data requiring protections (clinical trials, patient survey responses, etc.) as required by federal and non-federal sponsors.

The data above is hereafter referred to as "Confidential Data" in this policy.

POLICY STATEMENT:

Permissible Use

I. UConn Health *confidential or restricted data* is not authorized to be stored on either a UConn Health or non-UConn Health MCD unless all 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 requires a password for access and is encrypted using methods authorized by the UConn Health IT Department.

Institutionally-Owned Devices

I. MCDs will be provisioned using software and/or controls which will be defined by UConn Health IT Security and may include, but are not limited to:

1. Encryption of the device.

2. Use of a personal identification number (PIN) security pattern, password or other form of authentication as provided by the device manufacturer consisting of a minimum of four (4) characters or other form of authentication to gain access to the device.

3. Setting of an inactivity timeout of no more than 15 minutes requiring the password or PIN to be entered when the timeout is excluded.

4. Ability to initiate a remote "wipe" or deletion of data if a credible report is received that the device is lost or stolen.

Personally-Owned Devices

I. Users will be granted the authority to configure their personally-owned MCDs to access UConn Health electronic information, under the following conditions:

1. The user understands and agrees that such access is considered a personal convenience for the user and as such, UConn Health will not reimburse or otherwise compensate the user for any costs associated with such access. Such costs may include, but are not limited to, monthly call and data plans, long distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes.

2. Users agree to secure their wireless devices using software and/or controls which will be defined by UConn Health IT Security. These controls may include, but are not limited to, the following:
    a. If the device accesses UConn Health's *data of any type*:
        i. Use of a personal identification number (PIN) security pattern, password or other form of authentication as provided by the device manufacturer consisting of a minimum of four (4) characters or other form of authentication to gain access to the device.
        ii. Setting an inactivity timeout of no more than 15 minutes requiring the password or PIN to be entered when the timeout is exceeded.
        iii. External storage devices are excluded from i) and ii) above.

    b. If the device is used to access *confidential or restricted UConn Health data*, IT Security will ensure that the approved security controls, including encryption, are installed.
        i. External storage devices are included.

3. The user understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of the confidential information accessed and/or stored on the personal device.

4. Upon termination of affiliation with UConn Health, users agree:
    a. To immediately delete all institutional data stored on the device, excluding research data which will move with the MCD owner.
    b. To remove the UConn Health email account and WiFi settings from the device.
    c. Failure to complete the above may result in the device being auto-wiped by IT Security.

5. Users acknowledge that UConn Health does not provide support for personally-owned devices and has no liability for such devices. Configuration of any personally owned device is the user's responsibility.

6. Additional information about configuring devices can be found at: http://health.uconn.edu/information-technology

Additional MCD User Responsibilities

I. Users may not bypass or disable UConn Health-required security mechanisms under any circumstances.

II. Users are expected to take the appropriate precautions to safeguard their MCD against loss or theft.

III. Unauthorized physical access, tampering, loss or theft of an MCD must immediately be reported to UConn Health Public Safety in order to initiate effective and timely response and remediation of any possible breach of UConn Health data.

IV. Basic Science users who do not store confidential or restricted data may optionally use the device encryption software provided by the UConn Health IT Department.

Governance

I. Failure to adhere to this security policy and associated procedures may result in sanctions as per applicable UConn Health policy.

Thomas Murphy (Signed) 3/10/15

Thomas Murphy **Date**
Chief Information Security Officer

Iris Mauriello (Signed) 3/10/15

Iris Mauriello **Date**
Compliance Integrity/Privacy Officer

Andrew Agwunobi (Signed) 3/11/15

Andrew Agwunobi, M.D., M.B.A. **Date**
Interim Executive Vice President for Health Affairs

Replaces: Policy #2003-32 Portable Computing Device Security (4/14/03)
Revised: 05/27/08, 07/10/12, 3/12/13, 2/17/15