

UNC School of Medicine

Policy for Handheld Computing Devices

Scope

This policy applies to all “Handheld Computing Devices” including, but not limited to: Digital Organizers, Personal Digital Assistants, Smart Phones, Wireless E-mail Devices (Blackberry, Treo, etc.), and any other portable device used to store or access protected health information or other sensitive data. This policy does not apply to any devices, such as laptop computers, which are specifically covered under other policies. Any removable media used in conjunction with a handheld computing device should be safeguarded according to the appropriate policies on digital media. Compliance with this security policy is a requirement for all handheld computing devices storing or accessing protected health information on the University of North Carolina network.

General Guidelines

Handheld computing devices provide increasing levels of power, portability, and convenience to their users. Security measures used to safeguard protected health information should be reasonable and appropriate to the sensitivity of the information and the risk of a disclosure. Cumbersome security measures that discourage full compliance should be avoided.

Departments are encouraged to secure handheld computing devices that they control using network controlled or centrally managed software that provides a client/server model for policy change and enforcement on handheld computing devices.

When possible and appropriate, any health information should be stored on handheld computing devices in a de-identified form; where names, date of birth, social security numbers or other clear identifiers as outlined in the HIPAA regulations are not included with the information stored on the device.

Handheld Requirements

The following are specific technical requirements that must be satisfied by every handheld computing device storing or accessing protected health information or other sensitive information, including those purchased with personal funds. These requirements are general enough that any appropriate handheld computing device should be capable of compliance. Handheld computing devices used to process protected health information or other sensitive information must:

- require a power-on password. “Quick” passwords that are activated by pressing a sequence of function keys on the device are acceptable.
- be configured to log-off or power down no longer than fifteen (15) minutes after the last user activity.
- use encryption for all protected health information or other sensitive information that is stored on external media such as memory cards.
- require a minimum password length of five (5) characters or keys.
- provide a device reset (data erasure) if an incorrect password is entered more than five (5) consecutive times, when technically feasible.

Equipment Disposal

Prior to disposal or transfer, all handheld computing devices and associated memory cards must be completely cleared of all data in compliance with the School of Medicine Electronic Data Disposal Policy.

Exceptions

Exceptions to this policy will be strictly limited. In the event that a business need exists for a handheld computing device that is not capable of satisfying the above requirements, the School of Medicine's HIPAA Security Officer or designate, on a case-by-case basis, may provide exceptions to these requirements.

Reporting

Loss, theft, or any unauthorized use of a handheld computing device that has been used to store or access protected health information or other sensitive information constitutes a disclosure and must be reported to the departmental HIPAA Coordinator or the School of Medicine HIPAA Security Officer immediately.

Sanctions

Failure to comply with this policy may result in administrative sanctions in accordance with existing University policies, up to and including separation from the University.

Definitions

Sensitive Information. For purposes of this policy, Sensitive information is classified as PHI, Confidential Information or Internal information as defined in the UNC Health Care Information Security policy. For a full description of these security classifications, refer to the UNC Health Care Information Security policy.

PHI. Protected Health Information- Health information, including demographic information, created or received by the UNC Health Care System entities which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual.

References

- UNC Health Care Information Security Policy
- School of Medicine Electronic Data Disposal Policy

Authorship and Review

A subcommittee of the School of Medicine's HIPAA Security Team developed this policy. Questions, comments, or concerns regarding this policy should be directed to the School of Medicine's HIPAA Security Officer. This policy should be reviewed on an annual basis and all feedback provided on this policy will be considered during that review.

Approved by the HIPAA Planning and Oversight Council (HPOC): May 24, 2005