School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Portable Devices
HIPAA Policy Reference:	3.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

The nature of portable devices allows them to be easily carried outside SMPH space and used in uncontrolled environments, often without the user thinking about the consequences. As a result, potential loss or theft of portable devices poses a significant risk of breach of data. This policy addresses the appropriate use and disposal of all portable devices used for business purposes including those that are personally owned.

2. Definitions

2.1. *Portable computing devices:* Portable devices that are capable of storing, processing or collecting data including but not limited to notebook computers, handheld computers, tablet computers, portable digital assistants (PDAs) and smart phones.

2.2. *Portable media:* Any data storage media or device intended to be removed from its computing device. This includes, but is not limited to: CDs, DVDs, portable hard drives, USB external memory (memory sticks).

2.3. *Encryption:* Process used to render data unreadable to anyone not authorized to access it.

3. Policy

3.1. Storing PHI on any portable device is discouraged and should be avoided if at all possible.

3.2. No portable device used for business purposes may be shared with anyone unauthorized to access PHI, including family members.

3.3. All portable devices to be used for business purposes must be approved and registered with the departmental IT group and must be safeguarded from theft with the same care provided to a personal credit card. When feasible, portable devices should be labeled to facilitate recovery if lost. Any loss or theft of a device must be reported immediately to the departmental IT group or HIPAA Security Officer.

3.4. Portable media that cannot be safeguarded via encryption must be protected using additional physical security measures. Typically this only applies to storage media such as archival tape backups.

3.5. All notebook computers used for business purposes must be encrypted.

3.6. Other portable devices that are used in a way that stores data locally must be encrypted if technically possible. On devices that do not support encryption, other measures must be taken to protect against data breach such as strong password protection combined with a mechanism to remotely erase data.

3.7. Portable computing devices are subject to workstation security policy and must be kept up to date on operating system, antivirus, and all browser software.

3.8. When used in public areas, measures must be taken to ensure information on a portable device cannot be viewed by anyone not authorized to do so, and devices must not be left unattended.

3.9. All portable devices must be reviewed by departmental IT staff for disposal or removal of data when no longer used for business purposes. A documented data destruction method must be used on the device or media to render the data unreadable prior to disposal. Any non-magnetic removable media such as a CD or DVD no longer needed must be physically destroyed before being discarded.

4. Departmental Procedures

4.1. Each department must maintain an inventory of registered devices including either the method of encryption or the mechanism of securing the device when encryption is not possible.
4.2. Each department must maintain a procedure to address data erasure and/or destruction.

5. References

5.1. Related HIPAA Security Policies
- Workstation Use and Security
- Remote Access

5.2. UWHC Policy 1.06: Electronic Media Handling, Destruction, and Disposal
5.3. UW-Madison Electronic Devices policy: http://www.cio.wisc.edu/policies/devices.aspx