School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Workstation Use and Security
HIPAA Policy Reference:	4.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

All workstations with access to PHI are subject to the following safeguards to protect against the loss or disclosure of PHI.

2. Definitions

2.1. *Workstation:* A single user client computer used to access or process PHI
2.2. *Publicly accessible space:* A work area not physically separated (for example, by lockable doors) to areas that are commonly accessed by the general public.
2.3. *Shared space:* An area not generally shared with the public but used by more than one employee.

3. Policy

3.1. Workstation use must be restricted by some method of authentication such as password to restrict access to PHI. Automatic log-ins are not allowed. When available, the option to "remember password" in applications must not be used.
3.2. Any workstation in publicly accessible space or shared space must be configured be to either screen-blank or automatically log-off after some period of inactivity, not to exceed 15 minutes and the screen must be positioned to minimize inappropriate viewing of data. Any workstation used to access PHI in publicly accessible space must be secured by a physical anti-theft mechanism.
3.3. Users should log off all applications and the network, or use a workstation lock function before leaving a workstation unattended. When workstations are located in private offices, the office must be locked when unoccupied for any extended period. Care must be taken to restrict visual access to data displayed on the workstation by positioning screens appropriately. Workstations in private space must be configured to either perform a locking screen-blank or automatically log off after a period of inactivity, not to exceed 45 minutes.
3.4. Mechanisms must be in place to ensure that all workstations are secure with respect to operating system, software patches (including web browsers and plug-ins), anti-virus software, and anti-spyware software. Any machine containing PHI that is unable to be upgraded to current standards must be isolated from the rest of the network. Any workstation with known malware must be removed from the network and cleaned as soon as possible.
3.5. Storing PHI on computers outside of the office or clinic, such as home computers must be avoided. Users should consult with their IT staff which can provide remote access solutions that provide secure access to data if necessary. Any home computer that contains PHI must have the same workstation safeguards as an office/clinic machine and may not be shared with others that are not covered employees of the ACE.
3.6. All users must beware of attempts to gather personal information needed to access protected data. For example, users must not respond to solicitation of personal identity information including passwords. In the

case of troubleshooting password problems, work only with those known to be departmental IT staff. All users must reset their password after anyone else has changed it.

3.7. When it is determined that a storage device, either inside a computer or external to it is no longer to be used to store PHI, the device must be either cleaned of that data or destroyed. Similarly, when any computer or storage device is to be taken out of service, data storage components must be removed and the device disposed of according to departmental procedure (consult your departmental IT staff.)

4. Departmental Procedures

4.1. Each department must document the mechanisms used to secure workstations they administer including what steps are taken to protect workstations from malicious software and the method for disposing of obsolete data storage devices and media.

5. References

5.1. Related HIPAA Security Policies

- Password Use and Storage
- Server Security
- Remote Access

5.2. UW-Madison Electronic Devices policy: http://www.cio.wisc.edu/policies/devices.aspx

5.3. UWHC Administrative Policy 1.04: Workstation Acceptable Use and Security Management