POLICY:

Best Practices Regarding Workstation Configurations and HIPAA Security Guidelines Effective 4/20/05

1) **Password protected screen savers**
   - Screensavers should be set to 30 minutes or less and be password protected. If a computer is located in a common area visible by patients or other non-departmental personal, a more frequent timeout should be enabled (e.g., 5 minutes or less).

2) **Don’t store PHI or other sensitive data on the local workstation if possible**
   - All computers supported by AHC-IS provide the user with server disk space. The servers have added protection such as being behind a firewall and the data stored on the servers is backed up on a nightly basis.
   - Box.umn.edu is secure method to store and share sensitive and HIPAA related documents.

3) **Don’t post usernames/passwords on monitors, keyboards, etc.**

4) **Take precautions to secure the physical locations of machines storing private data**
   - Lock office doors when leaving for the day or not in use; laptops are required to be secured by a cable lock; consider dedicated printers/fax machines for printing of sensitive data and place in secure location; restrict placement of machines in common areas accessible by non-authorized staff wherever possible.

5) **Don’t leave PHI or other private data visible on monitors or desks**
   - Close computer documents when not in use or ensure screen savers are enabled (see item #1). Also, be aware of any hard copies of PHI or sensitive data that are kept on desks, around local printers, fax machines, etc. Make sure that hard copies are properly disposed of to prevent viewing by unauthorized staff, patients, etc.

6) **Ensure that anti-virus is installed and configured to update on a daily basis**
   - AHC-IS supported computers running Windows 7 or OS X or higher runs centrally managed anti-virus that is updated daily from the vendors website. See [http://it.umn.edu/anti-virus](http://it.umn.edu/anti-virus) if you need anti-virus software.

7) **Ensure that critical Windows software patches are installed.**
   - AHC-IS supported computers running Windows 7 are patched via central management software and Active Directory policies. AHC-IS supported computers running OS X are configured to check the vendors website daily for system updates. This service provides timely updates to the computers without user intervention.

8) **Turn off the computer at least once every 24 hours.**
Turning off your computer at the end of the day reduces the exposure to malicious attacks. Additionally, all computers should have password protection logon enabled to prevent unauthorized individuals from accessing after hours or while you are out of the office.

9) If you are using a wireless device such as a laptop, use the University Virtual Private Network (VPN) if possible.
   - Cisco VPN AnyConnect is installed on all AHC-IS supported machines.
   - VPN connections ensure connections are encrypted and reduce the risk of being viewed by malicious individuals. See [http://it.umn.edu/downloads-guides](http://it.umn.edu/downloads-guides) for additional information.

10) Avoid sending PHI or private data through email whenever possible.
    - Care should be taken to share PHI data via email in the event the receiver is reading it on a public computer or it is accidentally sent to the wrong recipient. Additionally, it is against University policy to send PHI to others beyond the University, University of Minnesota Physicians, and Fairview. See [http://www.policy.umn.edu/Policies/it/Use/ITRESOURCES_APPF.html](http://www.policy.umn.edu/Policies/it/Use/ITRESOURCES_APPF.html) for acceptable guidelines regarding PHI and email.
    - If email of PHI can not be avoided please use [ProofPoint](http://it.umn.edu/email-software-setup-guides) to email sensitive and PHI information.
    - Whenever possible, a web browser should be used to access University email. Clients such as Outlook or Thunderbird only be used if there is a critical business need for doing so and must be configured for secure connections. Accessing email via a smartphone or tablet must only be done if the device is configured according to University policies for devices in the Health Care Component (HCC). See [http://it.umn.edu/email-software-setup-guides](http://it.umn.edu/email-software-setup-guides) for more information.

11) All computer hardware and storage devices should be recycled though AHC-IS.
    - AHC-IS recycles devices in accordance with University policy. See University Policy [http://it.umn.edu/enterprise-standards/information-security-standards/media-sanitization](http://it.umn.edu/enterprise-standards/information-security-standards/media-sanitization)
    - Hard drives other and storage devices are destroyed, rendering them unusable for future use.
    - Computer hardware is recycled though the University recycling service and all obsolete equipment is removed from inventory (both University and AHC-IS inventories).