

**Subject:** AHC Standards for Technical Support

**Applicable to:** All AHC Servers, Workstations, Laptops,  
and Other Mobile Computing Devices

**Authors:** Ross Janssen, Privacy and Security Officer  
Terry Bock, Chief of Staff  
Steve Cawley, CIO

**Replaces version Dated:** NA

**Approved by** AHC Deans Council on April 25, 2006

---

**POLICY: Academic Health Center Standards for Technical Support of Servers, Workstations, Laptops, and Other Mobile Devices**

***Introduction***

HIPAA and University policies have established requirements for safeguarding protected health information (PHI). The Minnesota Data Practices Act now requires the University to notify individuals about any security breach that involves any private data about them, including PHI.

These standards establish the security and technical support requirements for Academic Health Center (AHC) servers, workstations, laptops and other mobile computing devices necessary to comply with University policies and state and federal data privacy and security laws. These standards are intended to be consistent with standards established by the University of Minnesota Office for Information Technology (OIT), but in some cases may be more restrictive than University standards. In instances where there is a difference between this policy and University policy, the stricter of the two policies shall apply.

The AHC requires a higher level of technical support and security because non-public data exists across all levels of the organization. This approach is consistent with University policy Academic/Administrative policy 2.8.1 - Acceptable Use of Information Technology Resources - Appendix M: Information Technology Support Guidelines states:

**" Continuity of support for private data:** Units that have a substantial portion of their activity involving access or storage of private or non-public electronic data should assume that the entire unit accesses or stores private data and that all electronic devices need to be secured. In such an environment, it is likely that access to (or physical transfer of) such data will occur on a regular basis."

These standards are needed to ensure data is available on a reliable basis and data integrity and security are not compromised. The ever increasing attacks from computer "hackers" require a high level of expertise and vigilance in protecting AHC servers, workstations, laptops, other mobile computing devices and associated data. This standard defines the management and support requirements for the use of servers, workstations, laptops, and other mobile computing devices by AHC workforce members and volunteers.

**Reason for Policy**

- To protect the privacy and provide for the security of individual health information in accordance with state and federal laws.
- To ensure an adequate level of technical support for the privacy and security of individual health information.
- To protect the University against damaging legal consequences.
- To assure the Academic Health Center has appropriate administrative and oversight mechanisms to facilitate compliance with all applicable laws and policies.

**Implementation of Standards**

- The standards set forth in this policy are effective immediately.
- Consolidation of technical support for AHC servers and workstations currently not supported by AHC IS will begin April 25, 2006, the effective date of this policy, and continue until completed.
- The order in which AHC schools or units will have their technical support consolidated into AHC IS will be prioritized based on risk factors and available resources.
- All technical support for AHC servers and workstations will be consolidated into AHC IS no later than December 31, 2007.

**Server Technical Support Standard**

- All AHC servers must comply with the AHC Server Standards (AHC IS Policy No. 9001) and University Policy.
- All AHC servers must be supported centrally by the Academic Health Center Office for Information Systems, (AHC IS), unless an exception is made as detailed below.

**Workstation Technical Support Standard**

- All AHC workstations and those who use them must comply with the AHC IS Workstation Standards (AHC IS Policy No. 9002) and all other applicable University standards.
- All AHC workstations must be configured to meet University and AHC security standards.
- University private data may not be stored on any personally owned workstation.
- All AHC workstations must be tracked according to AHC Workstation Standards.
- All workstations used by AHC workforce members and volunteers to perform work-related duties, must be purchased, configured, and supported by the Academic Health Center Office for Information Systems, (AHC IS).
- All University private data should be stored on an AHC IS server rather than on a workstation.
- Personally owned computers may be restricted from accessing AHC servers.

**Laptops and Other Mobile Computing Devices Technical Support Standard**

- All AHC laptops and other mobile computing devices and those who use them must comply with University and AHC standards.

- 
- The configuration of all AHC laptops and other mobile computing devices must meet University and AHC security standards.
  - University private data may not be stored on personally owned laptops or other mobile computing devices.
  - Laptops used by AHC workforce members and volunteers must be purchased, configured, supported, and tracked by AHC IS. All laptops gifted or otherwise provided by an entity external to the AHC must be configured by AHC IS and AHC IS must have administrative rights.
  - All University private data on AHC laptops must be encrypted to the level established by AHC-IS.
  - All AHC workforce members and volunteers must take steps to appropriately provide for the physical security of laptops and other mobile devices.
  - All AHC laptops must be physically secured with a cable lock.

### **Remote Site Technical Support Standard**

Many AHC units maintain remote sites where AHC workforce members and volunteers use AHC servers, workstations, laptops and other mobile devices. Remote sites are required to:

- Provide for connectivity through University Networking and Telecommunications Services (NTS) or the state network.
- Have their servers, workstations, laptops, and other mobile computing devices purchased, configured, and supported by AHC IS personnel.

### **Auditing and Monitoring Standard**

All AHC servers, workstations and mobile computing devices are subject to review for compliance with University and AHC standards.

### **Loss or Theft Reporting Standard**

Workforce members and volunteers must promptly report the loss or theft of any workstation or peripheral device. In addition workforce members should promptly report the loss or theft of any access device or mechanism such as a key, ID Card, door key, file key, etc that allows physical access to secure areas where workstations or other peripheral devices are located. .

To report a loss or theft:

1. Notify the University of Minnesota Police Department immediately by calling either 911 from a campus phone or 624-2677 (624-COPS).
2. Notify the Office of OIT Security and Assurance if you are reporting an incident that involves any private data theft (examples of private data include Social Security number, student records, private health information, etc). You may notify them using any one of the following three ways:
  - email [abuse@umn.edu](mailto:abuse@umn.edu)
  - call 1-HELP from a campus telephone
  - call 612-301-4357 from any other telephone
3. Notify the Privacy and Security office if the theft involves loss of any private health information. The Privacy and Security Office can be reached at 612-624-7447, or email

[privacy@umn.edu](mailto:privacy@umn.edu), or online at  
<http://www.ahc.umn.edu/privacy/contact/incidentreport/home.html>.

It is crucial that any incident that involves loss of private data be reported as quickly as possible. The Privacy and Security office has a legal obligation to log and track all HIPAA related incidents.

***Process for Requesting an Exception to This Standard***

Exceptions to the Academic Health Center Standards for Technical Support of Servers, Workstations, Laptops, and Other Mobile Devices must be approved by the University Privacy and Security Officer in consultation with the HIPAA Security Steering Committee.

***Documentation Requirements***

Documentation will be required for workstations, laptops and mobile computing devices that qualify as an exception to these standards.