School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Network Devices
HIPAA Policy Reference:	1.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

The data communication network which serves the UW School of Medicine and Public Health is functionally divided by department to provide a mechanism to restrict access to PHI. This policy addresses how the SMPH network will be maintained, when devices are allowed to connect to a network and when connections to a network may be disabled.

2. Definitions

2.1. *Network Device:* Any device, such as a computer, printer, or portable computing device, with either a wired or wireless connection to the SMPH network.

2.2. *Device Inventory*: A comprehensive list of each device which is connected to a departmental network. The description must include:

- Type of device
- Network (IP) address
- Hardware (MAC) address
- Host name or identifier
- Location if not a mobile device

2.3. *Network and Security Group (NSG):* The group given responsibility by the Dean's Office to oversee the operation and security of the network that serves the SMPH.

3. Policy

3.1. No network devices may be connected to any SMPH network without prior approval from either the departmental IT group which supports that network or the SMPH Network and Security Group.

3.2. No wireless access points may be connected directly to SMPH departmental networks. When wireless access is required only the campus UWNet or SMPH wireless networks may be used.

3.3. The NSG will administer perimeter firewalls which will restrict access to any departmental network containing PHI. Any requests for rules allowing access through departmental firewalls will include the purpose and name of contact.

3.4. Any network hosts that have associated firewall exceptions which allow access from the Internet will be periodically scanned for potential vulnerabilities.

3.5. Any publicly accessible data jacks must either be disabled, restricted to connect to specific devices, or on a network appropriate for public use (non-PHI).

3.6. The NSG will be responsible for automatically monitoring network traffic for activity that matches either an infected computer or a computer demonstrating known vulnerabilities. Based on level of threat, any computer detected to be compromised or at significant risk of compromise may be removed from the network and the associated IT group immediately notified.

4. Departmental Procedures

4.1. The NSG will maintain a set of standard procedures to address access controls, protocols, encryption techniques, vulnerability assessment and incident response.

4.2. The IT group in each department must maintain an inventory of devices connected to their network including the information in definition 2.2.

5. References

5.1. Related HIPAA Security Policies

- Workstation Use and Security
- Server Security

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