School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Server Security
HIPAA Policy Reference:	6.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

Departmental servers that store and/or transmit PHI must be secured in a way that safeguards the PHI to minimize the risk of data breach.

2. Definitions

2.1. *Server:* A physical or virtual computer which allows network connections from multiple users and:
- Is directly accessible from outside the UW Health network or,
- Shares one or more datasets containing PHI

2.2. *Data Center:* Locked physical space dedicated to housing servers and configured with appropriate cooling, power and fire suppressant. Access to data centers must be controlled and logged (e.g., use of a card reader or video logs).

2.3. *Server Inventory:* A list of all servers including the following:
- Domain name,
- Services it delivers,
- Type of computer,
- Physical location,
- IP address
- Operating system and release level.

2.4. *Unsupported Operating System:* Operating system not capable of security updates such as those no longer supported by the vendor.

3. Policy

Operations

3.1. Server administrator accounts and privileges must be restricted to those who need them to perform their jobs. Server administrators are subject to the same training and protocols as account holders, even if they are not given specific database authorization.

3.2. All servers must be maintained in such a way that the departmental IT group can ensure compliance with these policies including having administrative access.

3.3. All operating system and application software on servers must be maintained according to standards of good practice such as keeping software patches and virus definitions current.

3.4. Unsupported operating systems should not be run on servers. When an unsupported operating system must be run either departmental IT or NSG must be consulted so that the machine on which it is installed may be secured by other means.

3.5. Unneeded services must be disabled. For example, web hosting or email services must be disabled and blocked if the server is not intended to deliver them.
3.6. Servers must be secured and tested using industry-standard safeguarding tools such as the Center for Internet Security Benchmarks.

Physical Security

3.7. Servers should in all cases be housed in a data center as defined above. Servers that must be sited outside of data centers may do so only with approval from the Network and Security Group and must have other means of physical security.
3.8. Physical access to data centers must be restricted those needing access to fulfill their duties.

Server Transmission

3.9. When transmitting PHI outside of the secure network, the data and/or the connection must be encrypted.
3.10. Any server employing authentication for access control must pass all credentials in encrypted form. For example, all websites requiring log in must use SSL.

4. Departmental Procedures

4.1. Each department must document mechanism used to provide secure remote server administration.
4.2. Departmental IT must maintain an up-to-date inventory of all servers.
4.3. A description of the physical security used to protect servers (see 3.7).
4.4. Member(s) of the department must be designated to assure that all required operational procedures are carried out on a regular basis.

5. References

5.1. Related HIPAA Security Policies
- Password Use and Storage
- Workstation Use and Security
- Account Creation, Access Control and Auditing
- Disaster Recovery

5.2. Center for Internet Security Benchmarks: http://benchmarks.cisecurity.org