University of Wisconsin SCHOOL OF MEDICINE AND PUBLIC HEALTH

# HIPAA Security Policy

| | |
|---|---|
| **Policy Title:** | Remote Access |
| **HIPAA Policy Reference:** | 7.3 |
| **Effective Date:** | June 18, 2012 |
| **Status:** | Revision |

## 1. Purpose

Define standards for making secure connections to SMPH networks containing PHI from individual computers and other devices that are outside of the SMPH firewall including encryption and authentication.

## 2. Definitions

2.1. *PHI network segment:* An SMPH internal network segment which contains PHI and is secured by segregating it from other networks through the use of firewalls. Each clinical department has a separate PHI network segment.

2.2. *Remote Access:* Any connection from outside the SMPH network, including the Internet to resources inside the network. This includes both access to data on the network or data transmitted out of the network.

## 3. Policy

3.1. Remote access must be authorized by the department whose network segment is being accessed. Access must be restricted to those individuals who need such access in the course of their work.

3.2. Remote access connections must use some mechanism to authenticate users such as passwords.

3.3. Remote access mechanisms that transmit PHI via the Internet must secure all transmissions using a level of encryption approved by the department and sufficient to minimize the likelihood that an intercepted transmission could be decrypted.

3.4. It is the responsibility of anyone with remote access to the PHI network segment to ensure that the device being used complies with the *Workstation Use and Security* policy. Any device used for remote access must not be shared with anyone outside UW Health, not even family members.

3.5. Remote access using third-party proxy techniques (e.g. GotoMyPC, MyWebEx, LogmeIn) may be used only with departmental IT approval and may not be used for file transfers to computers not administered by the School of Medicine and Public Health.

3.6. Since online cloud services ( e.g., Carbonite, Dropbox, iCloud, Mozy) may allow for data to be copied from a PHI approved network to a network not controlled by UW Health, they are not acceptable for use. Users must consult with their departmental IT for remote file storage mechanisms.

3.7. Any staff outside of UWHealth needing access to data or devices on PHI network segments must have approval from that department and must work with the Network and Security Group to determine a secure mechanism to do so.

## 4. Departmental Procedures

4.1. Each department must document mechanism used to provide secure remote access to PHI network segments for departmental staff and others with access authorization.

## 5. References

5.1. Related HIPAA Security Policies

- Password Use and Storage
- Workstation Use and Security
- Account Creation, Access Control and Auditing

5.2. UWHC Administrative Policy 1.01: Remote Access to Electronic Information Systems