School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Disaster Recovery
HIPAA Policy Reference:	8.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

Each department in the SMPH that stores PHI or provides clinical services must develop a disaster recovery plan to address the possibility of significant loss of data or related service availability. The plan must include procedures in place which enable the restoration of data or critical clinical services in a timely fashion.

2. Definitions

2.1. *Disaster:* A sudden, unplanned event that significantly impedes the organization's ability to function as expected and to deliver the data and services that clients expect. Possible causes include environmental disasters (fire or flood), criminal activity (theft or vandalism), software tampering (malicious software destruction or data theft), and unexpected loss of personnel.

2.2. *Archive:* A snapshot copy of electronically stored data stored elsewhere with the original location, time and state of that data. In the event of a disaster an archive can be used to restore an IT system to a recent state.

2.3. *Disaster Recovery Plan (also known as "Contingency Plan"):* A written plan for recovering from an event categorized as a disaster. The goal of the plan is the rapid recovery of data, services and procedures. Such a plan should cover prevention measures, impact of loss of service, time and cost of recovery, notification and roles of personnel, technical procedures and testing.

2.4. *Off-site Backup:* A mechanism by which a copy of data can be stored at a site physically distanced from that at which the data is regularly stored.

3. Policy

3.1. Each department should develop and maintain a list of major data storage systems that house PHI and other data critical to business services.

3.2. All critical data including PHI must be backed up or archived on a regular basis. The back up mechanism must allow critical data to be restored as follows:

- daily for up to 30 days,
- monthly for up to 6 months and,
- semi-annually for 3 years.

3.3. Archives of critical data must be made at least monthly for off-site storage. Any data stored off site must be physically secured.

4. Departmental Procedures

Each department must submit annually to the HIPAA Security Officer:

4.1. Data Assessment: An estimate of the amount of PHI stored, the mechanism used to backup PHI, schedules for incremental and full backup, the location of off-site backup and procedures used to validate backups.

4.2. Disaster Recovery Plan: A set of written procedures for recovering data and services in the event of a disaster.

4.3. Business Continuity Plan: A description of any key clinical services provided and the procedure to be followed in the event of disruption to those services. This plan should include:

- The departmental IT personnel involved in recovery, methods for notifying them and their functions in the effort.
- Procedures for recovering data and reinstating services.
- Methods for testing the efficacy of the plan.

5. References

5.1. Related HIPAA Security Policies

- Server Security
- Account Creation, Access Control and Auditing

5.2. NIST Contingency Planning Guide: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=905266