School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Incident Response and Reporting
HIPAA Policy Reference:	10.2
Effective Date:	September 1, 2011
Status:	Original

1. Purpose

Establish requirements for responding to security incidents which may have resulted in the breach of sensitive information including PHI. This includes procedures for immediate response, evaluation of level of risk of data breach and appropriate reporting sequence.

2. Definitions

2.1. *Device:* Any electronic equipment that is capable of storing, processing or collecting data. This includes but is not limited to computers, printers, portable devices such as smartphones, and data storage devices.

2.2. *OCIS:* Office of Campus Information Security

2.3. *Security incident:* An event in which the confidentiality, integrity, or availability of sensitive information may have been compromised. Examples include the following: lost or stolen device, stolen credential such as a password, device compromised by malware or other means of remote entry, physical access to restricted areas by unauthorized personnel, or denial of service (DOS) attack which prevents a device from being properly accessed.

2.4. *Sensitive Information:* Institutional data that could, by itself or in combination with other such data, be used for identity theft, fraud, or other crimes. This includes PHI and other Personal Identifying Information (PII) as defined in the Wisconsin Breach Notification Law.

3. Policy

Initial Response to Incident

3.1. Any security incident must be reported immediately to the SMPH Network and Security Group.

3.2. In cases where it is known or is likely that a security incident is ongoing, steps must be taken to mitigate further risk of data breach. This may include removing a device's access to the network, blocking traffic from specific hosts, disabling an account or remotely disabling or erasing a portable device. Care must be taken to prevent the destruction of forensic evidence.

3.3. All thefts should be reported to the UW Police Department.

Assessment of Incident

3.4. The scope of the incident must be determined to verify that all devices, accounts, and datasets affected by the incident are included in the incident response.
3.5. The department IT group along with the Network and Security Group and the SMPH HIPAA Security Coordinator must conduct a preliminary assessment of any sensitive data that may have been put at risk. If it is likely that an incident has caused a breach of PHI then the UW-Madison HIPAA Privacy and Security Officers must be contacted. If any sensitive data is involved then the UW campus Incident Response procedure (5.3 below) must be followed.
3.6. After an assessment of the probability and extent of a data breach, the HIPAA compliance officers along with OCIS will develop a notification plan.

Remediation

3.7. The affected devices must be remediated, but only after relevant evidence has been collected. Remediation should only occur after consulting with the SMPH Network and Security Group or OCIS personnel. Examples of remediation include cleaning or rebuilding an infected computer, restoring erased or manipulated data from backup and in some cases changing a password.

3.8. In all cases, the cause of the security incident should be ascertained, and appropriate steps should be taken to prevent the same type of incident from recurring. For example, a machine compromised as a result of outdated software should be patched to the latest secure version.

4. Departmental Procedures

4.1. The Network and Security Group will maintain a set of procedures and tools to help departmental IT groups to assess and mitigate incidents.

5. References

5.1. Related HIPAA Security Policies
- Disaster Recovery
- Portable Devices

5.2. UWMF Security Incident Policy
5.3. UW-Madison Information Incident Reporting and Response Policy: http://www.cio.wisc.edu/policies/IReportPolicy.pdf
5.4. Definition of Sensitive Information: http://www.cio.wisc.edu/policies/SensitiveDataDefinition.pdf