University of Wisconsin-Madison
Policy and Procedure

Policy Number:	9.2
Policy Title:	Responding to Employee Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules
Effective Date:	March 15, 2004
Last Revision Date:	September 13, 2014
Page 1 of 5	

I. Policy

This policy addresses noncompliance by employees with UW-Madison's policies and procedures governing the confidentiality of protected health information under the HIPAA Privacy and Security Rules. For purposes of this policy, the term "employee" includes students in their role as employees (e.g., student hourly, student assistant). For example, a student who is employed as a student hourly to answer phones in a clinical department would be considered an employee.

It is the policy of UW-Madison to take appropriate steps to promote compliance with the requirements for maintaining the confidentiality of protected health information. UW-Madison takes seriously its requirements under HIPAA to protect the confidentiality of protected health information and will respond appropriately to violations of UW-Madison HIPAA policies and procedures.

The appropriate response to such violations will depend on a number of factors including the severity of the violation, the record of the employee, the applicable processes for the employment category, and whether another affiliated entity (e.g., University of Wisconsin Hospital and Clinics, University of Wisconsin Medical Foundation) is responding to the same violation by the same person. The response will be decided after investigating the specific facts of the situation and may include, but is not limited to, such actions as: system changes, additional education, a written reprimand, a suspension, and termination of employment.

Employees and others who are working in UW-Madison facilities who report, in good faith, violations of HIPAA policy requirements shall not be retaliated against. They may report any retaliation to their department chair/director, the dean/director, the Office of Human Resources or the UW-Madison Privacy Officer. If reported to anyone other than the Privacy Officer, it shall be referred to the Privacy Officer. The Privacy Officer shall determine who will investigate the matter.

II. Definitions

A. Protected Health Information ("PHI"): Health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the

individual. PHI does not include student records held by educational institutions or employment records held by employers.

III. Procedures

A. Many different categories of employees are covered under this policy. Therefore, it is the responsibility of the employee's dean or division director to determine the appropriate process to follow when aware of allegations of violations by an employee of UW-Madison's policies and procedures relating to HIPAA. If it is determined that a violation which could result in disciplinary action has occurred, the dean or division director, in consultation with the Office of Human Resources and the UW-Madison Privacy Officer, has the responsibility to determine the appropriate responses for employees other than faculty. It is expected that deans and division directors will initiate investigation of violations promptly and take action as appropriate. For faculty, the matter shall be referred by the dean or division director, in consultation with the Office of Human Resources and the UW-Madison Privacy Officer, to the provost for review when required under Faculty Policies and Procedures Chapter 9.

B. One of the factors to consider when determining the appropriate response for violations of UW-Madison's policies and procedures relating to HIPAA is the severity of the violation. UW-Madison has determined that there are four categories of violations.

1. Type I – these violations are inadvertent or accidental breaches of confidentiality that may or may not result in the actual disclosure of patient information (for example, sending/faxing information to an incorrect address).

2. Type II – these violations result from failure to follow existing policies/procedures governing patient confidentiality (for example, talking about patients in areas where others might hear, failure to obtain appropriate consent to release information, failure to fulfill training requirements).

3. Type III – these violations include inappropriately accessing a patient's record without a job-related need to know (for example, accessing the record of a friend or family member out of curiosity without a legitimate need to know the information).

4. Type IV – these violations include accessing and using patient information for personal gain or to harm another person.

C. In addition to the severity of the violation, factors such as the past record of the employee, the category of employment (see section D. below) and whether another covered entity (e.g., University of Wisconsin Hospital and Clinics, University of Wisconsin Medical Foundation, Meriter-Unity Point Health) is responding to the same violation by the same person must be considered. As a result, the appropriate response must be determined on a case-by-case basis. For example, while an inadvertent violation might normally result in additional education, it could result in more serious action if it was part of a pattern of violations or other performance problems.

D. Employees covered by this policy fall into different categories that have different policies, procedures, and laws covering their employment. For example, there are employees represented by unions as well as non-represented employees; among the non-represented employees, there are employees with civil service protections or tenure and there are at-will employees; there are classified employees covered by Department of Employment Relations' rules or collective bargaining agreements and unclassified employees covered by Regent Rules. Due to these complexities, deans and division directors should consult with the Office of Human Resources to ensure the appropriate process is followed for the particular employment category when investigating a possible violation and before deciding on the response to a violation.

E. All violations must be reported promptly to the UW-Madison Privacy Officer to determine, among other things, whether a breach has occurred that requires notification to patients or to the Department of Health and Human Services.

IV. Document Requirements

Any responses taken as a result of violations under this policy must be documented in a written or electronic record. This documentation must be retained by the UW-Madison Privacy Officer for six years from the date of its creation or the date when it was last in effect, whichever is later.

V. Forms

None.

VI. References

- 45 CFR 164.530 (e) (HIPAA Privacy Rule)
- 45 CFR 164.530 (j) (HIPAA Privacy Rule)

VII. Related Policies

- Policy Number 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information"
- Policy Number 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules"

VIII. For Further Information

For further information concerning this policy, please contact the UW-Madison HIPAA Privacy Officer or the appropriate unit HIPAA Privacy Coordinator or sub-Coordinator. Contact information is available within the "Contact Us" tab at hipaa.wisc.edu.

Reviewed By
Chancellor
Chancellor's Task Force on HIPAA Privacy
UW-Madison HIPAA Privacy Officer
UW-Madison Office of Legal Affairs

Approved By
Interim HIPAA Privacy and Security Operations Committee