This policy addresses noncompliance by students with UW-Madison’s policies and procedures governing the confidentiality of protected health information under the HIPAA Privacy and Security Rules.

This policy applies to students in a clinical health professional training program at UW-Madison who have access to protected health information. Students who access protected health information in their role as employees (e.g., a student who is employed as a student hourly to answer phones in a clinical department) would be considered an employee, not a student, for purposes of this policy. In this case, refer to Privacy Policy # 9.2 “Responding to Employee Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules.”

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 and the record of the student. 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, disciplinary probation, a suspension, and expulsion.

Students who are training 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 training program coordinator, department chair/director, the dean/director, the Dean of Students 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.

Applies to all members of the UW-Madison Health Care Component.
Rationale

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections apply over and above the new Federal privacy standards.

Policy Detail

Each school or college that educates students who will have access to PHI as part of their health professional training program will develop a school/college based disciplinary policy/procedure that is consistent with UWS Chapter 14 and/or UWS Chapter 17. The policy/procedure will, at a minimum, address the following.

1. An educational process by which students will be informed of the requirements of HIPAA and the consequences of not complying.

2. Progressive sanctions based on the severity of the violation and/or repetition of violations, recognizing at least the following four categories of violation:
   2.1 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).
   2.2 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).
   2.3 Type III – these violations include inappropriately accessing a patient’s record without a 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).
   2.4 Type IV – these violations include accessing and using patient information for personal use or gain or to harm another individual.

3. A process for notification of the office of the Dean of Students when the sanction recommended is to be documented in a student’s conduct file.

4. Automatic referral to the Dean of Students will occur if the violation is particularly egregious or repetitive in nature and the school/college would recommend disciplinary probation, suspension or expulsion.

5. 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.
Consequences for Non-Compliance

Failing to comply with this policy may result in discipline for the individual(s) responsible for such non-compliance.

Further, the US Department Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules, and an individual’s non-compliance may result in institutional non-compliance and/or an investigation by OCR. OCR attempts to resolve investigations by obtaining voluntary compliance and entering into Corrective Action Plans and Resolution Agreements. Failures to comply with HIPAA or cooperate with OCR in an investigation may result in civil and/or criminal penalties.

Supporting Tools

Additional information may be found at www.compliance.wisc.edu/hipaa

Definitions

1. **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.

Responsibilities

HIPAA Privacy Officer
HIPAA Security Officer

Link to Current Policy

[TBD]

Link to Related Policies

https://compliance.wisc.edu/policies-and-forms/

Link to Policy History

N/A

Review / Approval

- HIPAA Executive Board, March 26, 2020