HIPAA PRIVACY, SECURITY AND BREACH NOTIFICATION POLICY

SLT 8.6

Date of Last Update:
March 13, 2026

Approved By:

- Senior Leadership Team

Responsible Office:
Human Resources

POLICY STATEMENT

Grand Valley State University (“the University”) is a Hybrid Entity with designated Health Care Components, as defined under the Health Insurance Portability and Accountability Act (“HIPAA”). This Policy establishes a Breach Notification Policy for use in the event of a potential Breach or other security incident related to personal health information, as required under HIPAA and related amendments and implementing federal regulations.

The list of University designated Health Care Components, and definitions also applicable to this Policy, can be found here: University Disclosures. Only Covered Components can engage in HIPAA covered activity. Any University personnel or unit that is not designated as a Covered Component must obtain approval from the HIPAA Privacy Officer before engaging in any covered activity. The Designation List will be reviewed and updated at least every two years or as needed by the Office of General Counsel.

This Policy applies to all University personnel who work in, for, or with GVSU units that are designated as a Health Care Component.

POLICY

I. Organizational Guidelines

A. University personnel will maintain the privacy and security of PHI. The University will implement policies and procedures as necessary to comply with HIPAA and related laws, rules, or regulations.

B. The HIPAA Privacy Officer is the University's chief point of contact with the U.S.

Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for all HIPAA complaints, investigations, and related matters.

C. The HIPAA Security Officer will work with Covered Components to develop, implement, and maintain policies and procedures necessary for Covered Components to comply with the HIPAA Security Rule, including those necessary to establish and maintain administrative, physical, and technical security safeguards and to prevent, detect, contain, and correct security violations.

D. The Office of General Counsel, in consultation with HIPAA Privacy Officer, will periodically evaluate Covered Components, with input from appropriate stakeholders, to ensure that designations remain proper and any additional designations are made in a timely manner.

E. Other University units that provide health care services, while not subject to HIPAA privacy and security requirements, must comply with the University's privacy and confidentiality policies. In the event any other University unit receives notification of a potential HIPAA violation or violation of this policy, the unit shall promptly notify the HIPAA Privacy Officer.

II. Investigation

A. If a Covered Component identifies or is informed of a potential Breach or Security incident, they will promptly inform the HIPAA Privacy Officer and will cooperate with the HIPAA Privacy Officer, or their designee, throughout the initial fact-finding investigation and will provide all potentially relevant documents.

B. The HIPAA Privacy Officer and HIPAA Security Officer will evaluate the results of the initial investigation and work together to recommend appropriate corrective actions as necessary, including but not limited to notification under HIPAA or state or federal law. The HIPAA Privacy Officer may involve other University units as appropriate to conduct a full investigation, including, but not limited to legal counsel, employees, agents, contractors, or consultants.

C. All Workforce members will cooperate in such investigations and promptly respond to inquiries from the HIPAA Privacy Officer or HIPAA Security Officer, or to any other such requests from units assisting with or coordinating the investigation.

III. Breach Determination

A. For purposes of this Policy, a Breach is presumed if there is unauthorized access, acquisition, use, or disclosure of unsecured PHI. The presumption is rebutted if the University can demonstrate that (1) there is a low probability that the information was

compromised based on a risk assessment of certain factors set forth in the University's HIPAA procedures, or (2) the situation fits within one of the following circumstances or exceptions to the Breach notification rule identified above.

B. If the HIPAA Privacy Officer determines the information did not meet one of the circumstances or exceptions listed above, the HIPAA Privacy Officer must conduct a risk assessment. There is a presumption that an impermissible use or disclosure is a Breach unless it can be determined through a risk assessment that there is a low probability that the PHI has been compromised. If the HIPAA Privacy Officer concludes there is a low probability the PHI has been compromised, then notification is not required.

C. The University has designated a Breach Notification Team to assist the HIPAA Privacy Officer in evaluating the University's breach notification requirements. The team consists of:

1. Director (or equivalent) of the Covered Component where the violation may have occurred;

2. HIPAA Security Officer and member(s) of the Information Technology Security Team;

3. Representative from the Office of the Vice President for Business and Finance;

4. Representative from the Office of the General Counsel;

5. HIPAA Privacy Officer; and

6. Vice President, or their authorized representative, of the University Division where the potential violation occurred (if not already represented).

D. If the Breach Notification Team determines that the University must provide notification of an incident, the HIPAA Privacy Officer will prepare and send appropriate notification as set forth in the Breach Notification Procedures.

E. In determining whether notification is required, the HIPAA Privacy Officer may consult with legal counsel, employees, agents, contractors, consultants as reasonably necessary to determine the University's notification obligations.

IV. Business Associates

A. The University must have current, signed Business Associate Agreements (BAAs) with all entities that use or disclose PHI on behalf of the University or that provide services to a Covered Component.

B. Only the HIPAA Privacy Officer has authority to sign BAAs on behalf of the University's

Covered Components.

C. The University shall seek to require any Business Associate to notify the University of a potential breach within five business days of discovery and provide information about the individuals involved in the potential breach within thirty days of discovery.

D. In certain circumstances, Business Associate's knowledge of a breach may be imputed on the University. Therefore, the deadline for providing notice will be based upon when the Business Associate knew or should have known about the breach.

V. Reporting Violations

A. If any Workforce Member becomes aware of an actual or alleged violation of HIPAA requirements or this Policy, the individual shall report the actual or alleged violation as set forth in the Breach Notification Procedures. Any member of the public may notify the HIPAA Privacy Officer of an actual or alleged violation of HIPAA requirements or of this Policy.

B. The HIPAA Privacy Officer will make the final determination regarding whether a reported violation constitutes a Breach.

C. As required by applicable law, the University will mitigate any Breach, violation of this Policy or applicable HIPAA requirements.

VI. Exceptions

A. There are no exceptions to this Policy for Covered Components or Workforce Members.

B. Student health information obtained or created as part of the student's academic career is generally covered under the privacy provisions of the Family Educational Rights and Privacy Act (FERPA) and is kept separate from their medical records. This Policy in no way affects the applicability of FERPA regulations to student records, including student health records originally created as a result of health care services provided by the Campus Health Center or other campus clinics, programs, or centers, but that have been subsequently associated with the student's academic or conduct files.

VII. Accountability

A. Failure to follow this Policy and any associated procedures, including cooperating with any investigation or notice requirements, may subject University employees to disciplinary action, up to and including dismissal from employment by the University, consistent with applicable University policies and procedures.

B. Students in violation of this Policy may be subject to disciplinary action under the

applicable student policies and procedures.

C. Individuals who are in violation of HIPAA regulations may be subject to civil and criminal penalties as provided by law.

D. Retaliation of any kind (including but not limited to threats, intimidation, coercion, harassment or discrimination) against an individual who reports potential violations of this policy and/or HIPAA is prohibited. Individuals who believe that they have been retaliated against may submit a report here: Anonymous Report and/or file a complaint with any of the following:

1. U.S. Department of Health and Human Services Office for Civil Rights

2. U.S. Equal Employment Opportunity Commission

DEFINITIONS

I. Unless otherwise defined herein or in GVSU's designation page, all capitalized terms in this Policy have the same definitions found in HIPAA.

A. Breach: the acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164 subpart E which compromises the security or privacy of the protected health information.

1. Breach Excludes:

a. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under 45 CFR 164 subpart E.

b. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under 45 CFR 164 subpart E.

c. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such

information.

2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164 subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the protected health information or to whom the disclosure was made;

c. Whether the protected health information was actually acquired or viewed; and

d. The extent to which the risk to the protected health information has been mitigated.

B. Business Associate: A person or entity, other than a member of a Covered Entity's workforce, that performs a function or service on behalf of a Covered Entity that involves the use or disclosure of PHI. A Business Associate may be a department within the entity or an unaffiliated third party.

C. Covered Entity: A health plan, a health care clearinghouse, or a health care provider that transmits PHI in electronic form to conduct one or more of the following transactions: (i) claims, (ii) benefit eligibility, (iii) referral authorization, (iv) enrollment, (v) claim status, (vi) health care premium payments, or (vii) coordination of benefits.

D. HIPAA Privacy Officer: designated individual who works with Covered Components to oversee ongoing activities related to the University's implementation of this Policy.

E. HIPAA Security Officer: Individual or team who is responsible for ensuring compliance with the Security and Breach Notification Rules established at 45 CFR Parts 162 164, Subparts C and D.

F. Protected Health Information ("PHI"): individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

G. University Designated Health Care Components ("Covered Component"): Any University unit, or portion thereof, that meets the HIPAA definition of a Covered Entity or Business Associate if it were a separate legal entity shall be

designated as a Covered Component. The University's Designation of HIPAA Health Care Components identifies the Covered Components.

H. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

I. Workforce Member: any University employee, partner, volunteer, trainee, and/or agent of a University designated HIPAA Covered Component.

RELATED LINKS

GVSU Designation of HIPAA Health Care Components

Standards of Conduct Policy for Employees

Student Code: The Anchor of Student Rights and Responsibilities

Privacy of Individually Identifiable Health Information, 45 CFR 164 subpart E