Policy 1343
Title: HIPAA Compliance and Hybrid Entity Designation

Date of Current Revision: May 2025
Primary Responsible Officer: Provost and Vice President of Academic Affairs

1. PURPOSE

This policy is to establish the university's framework for compliance with the Health Insurance Portability and Accountability Act of 1996, as amended, and related regulations to the extent applicable to James Madison University. This policy also designates James Madison University as a hybrid entity under HIPAA and designates certain university components as health care components.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia section 23.1-1602; 23.1-1301. The board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATUTES AND /OR REGULATIONS
Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and related regulations including the Privacy and Security Regulations at 45 CFR §§ 160 and 164 (hereinafter collectively, "HIPAA"); Virginia Code §32.1-127.1:03, §2.2-3800 et seq.

3. DEFINITIONS

Access
The ability to read, enter, copy, query, download or update individually identifiable health information.

Breach
As defined by HIPAA at 45 CFR §164.402, the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR Part 164, Subpart E that compromises the security or privacy of the PHI.

Business Associate
As defined by HIPAA at 45 CFR §160.103, a business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information;
(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity; or
(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

A business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual;
(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of §164.504(f) of this subchapter apply and are met;
(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law; or
(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Contact Person
The position is designated to receive complaints under this policy and provide further information about matters covered by the university's Notice of Privacy Practices.

Covered Function
Any function the performance of which makes the entity a health care provider.

Covered Entity
As defined by the HIPAA regulations at 45 CFR §160.103, a (1) A health plan; (2) A health care clearinghouse; or (3) A health care provider who transmits any health information in electronic form in connection with a covered transaction.

Covered Entity Components
Any component that would meet the definition of a covered entity if it were a separate legal entity.

Covered Transaction
As defined by HIPAA at 45 CFR §160.103, the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information
(2) Health care payment and remittance advice
(3) Coordination of benefits
(4) Health care claim status
(5) Enrollment and disenrollment in a health plan
(6) Eligibility for a health plan
(7) Health plan premium payments
(8) Referral certification and authorization
(9) First report of injury
(10) Health claims attachments
(11) Health care electronic funds transfers (EFT) and remittance advice
(12) Other transactions that the Secretary may prescribe by regulation

HIPAA Compliance Committee
The HIPAA Compliance Committee is responsible for designating and identifying the JMU departments and units that are covered units and thus subject to HIPAA, based on performance of covered functions, and these shall be maintained by the HIPAA privacy officer.

Compliance Committee Position	JMU Employee Assigned to the Position
HIPAA Contact Person	JMU IIHHS Associate Director of Clinical Services
HIPAA Privacy Officer	JMU IIHHS Associate Director of Clinical Services
HIPAA Security Officer	JMU IT Information Security Officer

HIPAA Contact Person or Office
A contact person or office who is responsible for receiving complaints regarding HIPAA and this policy, and is able to provide further information about matters covered by the Notice of Privacy Practices. 45 CFR 164.530(a)(1)(ii)

HIPAA Privacy Officer
An individual employee responsible for development and implementation of the general policies and procedures required by HIPAA and for the university's HIPAA Compliance Program. 45 CFR 164.308(a)(2); 45 CFR.530(a)(1)

HIPAA Security Officer
An individual employee responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C, regarding security standards for the protection of electronic PHI.

Health Care Component
Any component that would meet the definition of a covered entity or business associate if it were a separate legal entity; any component that accesses PHI for research purposes; and any component that is a business associate of an external covered entity. James Madison University designates the health care components (the components subject to HIPAA) as set forth in Attachment A.

Healthcare Provider
As defined by HIPAA at 45 CFR §160.103, a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Hybrid Entity
As defined by HIPAA at 45 CFR §164.103, a single legal entity that is a covered entity whose business activities include both covered and non-covered functions, and that designates health care components in accordance with 45 CFR §164.105(a)(2)(iii)(D).

Individually Identifiable Health Information
As defined by HIPAA at 45 CFR §160.103, information that is a subset of health information, including demographic information collected from an individual, and

- is created or received by a health care provider, health plan, employer or health care clearinghouse; and
- relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, or future payment for the provision of health care to an individual; and
- identifies the individual; or
- there is a reasonable basis to believe the information can be used to identify the individual.

Internal Business Associates
Certain university components, to the extent they provide business associate services to those in the course of the covered entities' health care provider treatment, payment and operations, or health plan actions under HIPAA. Internal business associates are set forth in Attachment A.

Notice of Privacy Practices
As defined by HIPAA at 45 CFR §164.520, the Notice of Privacy Practices ensures that an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the hybrid entity, and of the individual's rights and the hybrid entity's legal duties with respect to protected health information. A Notice of Privacy Practices must meet the requirements of 45 CFR §164.520(b).

Protected Health Information (PHI)
As defined by HIPAA at 45 CFR §160.103, protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii)Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:
(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) In employment records held by a covered entity in its role as employer; and
(iv) Regarding a person who has been deceased for more than 50 years.

For the purposes of this policy, the records described in Paragraph (2)(i) will be called "Education Records" and the records described in Paragraph 2(ii) will be called "Treatment Records."

Research
As defined by HIPAA at 45 CFR §164.501, research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

University Components
A component of the university, to include college, department, academic unit, program, institute, center, clinic, office, or function.

Workforce
As defined by HIPAA at 45 CFR §160.103, workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the university, is under the direct control of the university, whether or not they are paid by the university.

4. APPLICABILITY

This policy applies to the university, its components, and its workforce. The university's designated health care components are subject to university policy guiding adherence to HIPAA, including HIPAA's privacy and security rules. This policy most specifically applies to health care components and their workforce members, and university components that provide services necessary for HIPAA compliance.

5. POLICY

5.1 Hybrid Entity Designation

The university is a single legal entity that is a covered entity and that conducts both covered and non-covered functions under HIPAA. HIPAA allows the university to elect to be a hybrid entity with identified health care components that are subject to HIPAA's privacy, security, breach notification, and enforcement provisions. This policy designates the university as a hybrid entity under HIPAA, and designates as health care components those components that would meet the definition of a covered entity if it were a separate legal entity ("covered entity components") and those that would meet the definition of a business associate if it were a separate legal entity based on the creation, receipt, maintenance, or transmission of Protected Health Information (PHI) for one or more covered entity components ("internal business associates"). Health care components are set forth in Appendix A.

5.2 New Healthcare Component Status for a University Component

Any university component or workforce member who undertakes a new activity that would make that member a healthcare provider, business associate, or otherwise subject to HIPAA must notify the privacy officer before engaging in the activity.

5.3 Periodic Reviews

The university will conduct periodic reviews to revise, as necessary, health care component designation(s).

5.4 Compliance, Generally

Notwithstanding the hybrid entity designation, the university remains responsible for the HIPAA compliance to the extent applicable to the university, and specifically for the HIPAA compliance of its health care components. All health care components must maintain HIPAA compliance.

6. PROCEDURES

6.1 Health Care Component Compliance Required

All health care components are subject to and must ensure compliance with applicable HIPAA requirements, including, without limitation, the requirements of the HIPAA privacy and security rules. In particular, and without limiting this requirement, health care components must ensure that they adhere to the requirements below.

a. Do not disclose PHI to another component of the university in circumstances in which the HIPAA Rules at 45 CFR Part 164, Subpart E would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;
b. Protect electronic PHI with respect to another component of the university to the same extent that it would be required under 45 CFR Part 164, subpart C to protect such information if the health care component and the other component were separate and distinct legal entities; and
c. If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the university in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of or incident to the member's work for the health care component in a way prohibited by 45 CFR Part 164, subpart E.
d. Develop operating procedures and forms as needed for HIPAA and HIPAA-related policy compliance. Health care components must provide the privacy officer with current copies of any such documents.
e. Train all of their workforce members on policies and procedures, including with respect to PHI, as required by the HIPAA rules and as necessary and appropriate for the members of the workforce to carry out their functions within the health care component. Training must be provided in the following circumstances: to each workforce member by no later than the compliance date for the covered entity; thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and to each workforce member affected by a material change in the HIPAA-related policies or procedures within a reasonable period of time after the material change becomes effective. All health care components shall maintain copies of the training materials and document that the required training was provided and to whom on what dates. All training documents, including attendance rosters, must be timely forwarded to and maintained by the HIPAA privacy officer.

6.2 JMU Information Technology

The information technology department, in collaboration with the HIPAA security officer, will provide the information technology services and support necessary for HIPAA compliance. These services and support include, but may not be limited to, compliance with HIPAA’s technical requirements; regular monitoring, analysis, and testing of the university network; and verification of the security controls of systems authorized to interact with PHI.

6.3 Institutional Review Board for the Protection of Human Research Participants (IRB)

The university IRB also acts as the Privacy Board to provide HIPAA Privacy Rule review and documentation for researchers that seek to use and/or disclose PHI. This includes approval/disapproval of waivers or alterations of HIPAA; review combined consent/authorizations; receipt of HIPAA attestations from investigators; provision of template HIPAA-related forms; and other research-related activities as required by HIPAA.

See also JMU Policy 1104 - The Institutional Review Board on the Use of Human Subjects in Research.

6.4 HIPAA Privacy Officer

The HIPAA privacy officer is an individual employee responsible for development and implementation of the general policies and procedures required by HIPAA and for the university's HIPAA compliance program. (45 CFR 164.308(a)(2); 45 CFR 164.530(a)(1)). The privacy officer's responsibilities include, but are not limited to the following:

a. The development, website posting, and implementation oversight of the HIPAA compliance procedures for health care components. The HIPAA privacy officer may require a health care component to change its procedures, forms, or related documents to ensure HIPAA compliance
b. Determining whether the status of a university component should change to or from that of a health care component and ensuring Appendix A is updated.
c. Breach procedures and notification, including receipt of reports of potential, suspected, or actual breaches.
d. Serving as the HIPAA contact person responsible for receiving complaints regarding HIPAA-related matters, and who is able to provide further information about matters covered by the Notice of Privacy Practices. (45 CFR 164.530(a)(1)(ii).

6.5 HIPAA Security Officer

The HIPAA security officer is an individual employee responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C regarding security standards for the protection of electronic PHI.

6.6 HIPAA Compliance Committee

The HIPAA Compliance Committee assists the HIPAA privacy officer in the adoption and implementation of policies and procedures for university HIPAA compliance. The HIPAA Compliance Committee will include, but is not limited to, the following: The HIPAA privacy officer, the HIPAA security officer, the HIPAA contact person, or a representative of the HIPAA Contact Office. The committee shall meet at least two times each year.

6.7 Breach Reporting

All employees are required to report any potential, suspected, or actual breach of PHI immediately to the HIPAA privacy officer. Some examples of breaches include, but are not limited to:

- Loss or theft of a laptop, external hard drive, thumb drive or paper chart containing PHI;
- Access to PHI outside of an individual's job responsibilities;
- Improper disposal of PHI such as failure to shred paper documents or securely delete electronic records prior to device disposal or repurposing;
- Misdirected mailings, emails, faxes, or other communications; or
- Malware infection on ePHI containing devices

6.8 Business Associate Agreements

a. Procurement Services and health care components are responsible for identifying when a vendor/external entity is a business associate and ensuring that a Business Associate

Agreement (BAA) is properly entered into and the document is maintained. BAAs that are provided by the vendor or that require negotiation must be reviewed by the Office of University Counsel before being signed.

b. A university component that is not a health care component must notify the HIPAA privacy officer prior to entering into an agreement that will require the university to provide business associate services to an internal or external covered entity. A university component or workforce member may not provide or agree to provide business associate services unless the relevant university component is designated as a health care component in Appendix A. BAAs that are provided by the vendor or that require negotiation must be reviewed by the Office of University Counsel before being signed.

6.9 Complaints

Complaints concerning HIPAA policies and procedures and/or compliance with those policies and procedures must be made in writing to the contact person. The contact person will investigate all complaints in a timely manner and provide a written determination to the parties involved (e.g., the complainant and the healthcare components) and to the HIPAA privacy officer (if the contact person and privacy officer are different individuals). The HIPAA privacy officer may confer with appropriate university administrator(s) to recommend sanctions, as appropriate, and to propose amendments to policies and procedures, as needed.

7. RESPONSIBILITIES

All departments, offices and employees that generate, receive, or maintain public records under the terms of this policy are also responsible for compliance with Policy 1109 – Records Management.

8. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment, suspension or expulsion from the university, or termination of affiliation/business association with the university.

9. EXCLUSIONS

None

10. INTERPRETATION

The authority to interpret this policy rests with the president and is generally delegated to the provost and vice president of academic affairs.

Previous version: N/A
Approved by the president: May 2025

Appendix A: Health Care Components

Covered Entity Components
The following covered entity-like university components are health care components of James Madison University, to the extent that Educational Records subject to and treatment records excluded from the Family Educational Rights and Privacy Act are not involved, and to the extent that payment is collected via HIPAA-covered billing:

- Athletics
- Audiology Clinic
- Speech-Language Clinic
- Occupational Therapy Clinical Education Services
- Alvin V. Baird Attention and Learning Disabilities Center
- Interprofessional Autism Clinic
- Counseling and Psychological Services
- Interprofessional Services for Learning Assessment
- Rural Health Psychology Clinic
- Healthcare for the Homeless, Suitcase Clinic
- IIHHS Faculty Practice
- IIHHS Clinical Services

Internal Business Associates
The following business associate-like university components are health care components of James Madison University:

- Cash & Investments
- Facilities Management
- Information Technology Services
- Institute for Innovation in Health and Human Services – Clinical Services Billing
- Office of University Counsel
- Parking Services
- University Business Office
- University Communications