

 <b>UNIVERSITY OF DENVER</b>	<b>UNIVERSITY OF DENVER POLICY MANUAL HIPAA POLICY</b>	
<b>Responsible Department:</b> Enterprise Risk Management <b>Recommended By:</b> HIPAA Steering Committee <b>Approved By:</b> Chancellor	<b>Policy Number</b> RISK 12.10.030	<b>Effective Date</b> 4/3/2024

## I. INTRODUCTION

- A. The University of Denver (University) strives to protect the confidentiality, integrity and availability of protected health information (PHI) by taking reasonable and appropriate steps to address the requirements of the [Health Insurance Portability Privacy Accountability Act of 1996, Pub. L. No. 104-191 \(1996\)](#) (HIPAA).
- B. HIPAA regulates Covered Entities; which are health plans, health care clearinghouses and health care providers who transmit any Health Information in electronic form in connection with a Covered Transaction. HIPAA requires that each Covered Entity maintains reasonable and appropriate administrative, technical and physical safeguards for privacy and security. HIPAA also requires that entities or individuals who contract to perform services for a Covered Entity with access to PHI (referred to as “business associates”) comply with the HIPAA privacy and security standards.
- C. The University is comprised of multiple and distinguishable schools, departments, clinics, programs, and functions, some of which may conduct both Covered Transactions under HIPAA and non-covered functions .
- D. This Policy:
1. designates the University as a Hybrid Entity under HIPAA;
  2. identifies University Covered Components;
  3. identifies PHI Partner Members, which are non-covered components that follow HIPAA best practices;
  4. establishes the University HIPAA Steering Committee;
  5. designates the University HIPAA Privacy Officer; and

6. designates the University HIPAA Security Officer.

## II. POLICY OVERVIEW

### A. The University as a Hybrid Entity

1. **Hybrid Entity:** The University is a Hybrid Entity, which means that only certain components (schools/departments/units) have operations that meet the definition of Covered Entity to which HIPAA applies. The University Statement of Designation as a Hybrid Entity is attached as **Exhibit A**.
2. **HIPAA Covered Components:** A HIPAA Covered Component is an area of the University that serves as a health care provider, health plan, or health care clearinghouse that transmits Health Information electronically in connection with financial or administrative activities. These operations prompt compliance obligations under HIPAA. The University has identified the schools, departments, clinics, programs, or functions identified on the University Statement of Designation as a Hybrid Entity (attached as **Exhibit A**) as Covered Components because they either:
  - a. meet the definition of a Covered Entity, if each were a separate legal entity; or
  - b. are a University Business Associate.

**B. PHI Partner Members:** A PHI Partner Member is an area of the University that may encounter personal health information (PHI) in their job functions, but they do not meet the definition of Covered Entity and therefore are not subject to HIPAA requirements. Employees and others within these schools, departments, and units are called “PHI Partner Members.” PHI Partner Members:

1. are required to practice safe handling and use of PHI in accordance with this Policy; but
2. may not hold themselves out as a HIPAA Covered Component.

*Note:* PHI Partner Members do not include University departments or units that may encounter health information in records that are by definition either: (a) “education records” under FERPA (e.g. Office of Equal Opportunity and Title IX, Disability Services) or (b) “employment records” (e.g. Human Resources & Inclusive Community) and as such are not subject to HIPAA.

**C. HIPAA Steering Committee.** The University’s HIPAA Steering Committee is comprised of representatives from each of the Covered Components and PHI Partner Members as identified on **Exhibit A** - Statement of Designation as a

Hybrid Entity. The HIPAA Steering Committee is responsible for:

1. reviewing the University's Covered Components on an annual basis, and where appropriate, adding or removing Covered Component designations;
2. designating each of the University's HIPAA Privacy Officer and HIPAA Security Officer; and
3. serving as the governing authority to create, implement, and maintain HIPAA Privacy and Security Standards and Procedures

### **III. PROCESS OVERVIEW**

#### **A. Covered Component Responsibilities**

1. All Covered Components are subject to and must comply with applicable HIPAA requirements, including, without limitation, the requirements of the HIPAA Privacy Rule and HIPAA Security Rule.
2. Covered Components may only use and disclose PHI to a University non-health care component to the same extent, and in the same manner, as it is permitted to use or disclose PHI to individuals or entities that are legally separate from the University.
3. Covered Components shall provide compliance reports to the HIPAA Privacy Officer on a periodic basis. Such compliance reports will be facilitated via annual risk assessment conducted by the University.

#### **B. PHI Partner Members Responsibilities**

1. PHI Partner Members are responsible for maintaining the confidentiality of their clients' health information and the safe use and handling of PHI; and
2. completing training on their responsibilities with respect to PHI.

#### **C. HIPAA Privacy Officer Responsibilities**

The responsibilities of the University HIPAA Privacy Officer are to:

1. Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security related policies and procedures;
2. Conduct various risk analyses, as needed or required;

3. Appoint a Privacy Officer designee for each covered department/unit as appropriate;
4. Manage breach notification investigations, determinations, and responses, including breach notifications;
5. Coordinate with the HIPAA Security Officer to develop or obtain appropriate privacy and security training for all workforce members, as appropriate; and
6. Provide regular reports apprising the HIPAA Steering Committee of HIPAA-related compliance activities.

**D. HIPAA Security Officer Responsibilities**

The responsibilities of the University HIPAA Security Officer are to:

1. Develop appropriate policies, standards, guidelines, and procedures for information security systems;
2. Develop an incident management plan;
3. Manage technical systems to maintain the confidentiality, integrity, and availability of the University's information systems;
4. Monitor internal audits that assess the status of Covered Entities' HIPAA compliance;
5. Coordinate with the HIPAA Privacy Officer;
6. Develop or obtain appropriate security training for all workforce members, as appropriate;
7. Conduct regular risk analysis to identify potential vulnerabilities in the university's electronic systems and ePHI;
8. Develop and implement a risk management plan, implement security measures, and evaluate and maintain those security measures;
9. Continuously monitor the University's adherence to HIPAA security standards; and
10. Provide regular reports apprising the HIPAA Steering Committee of HIPAA-related security activities.

## E. HIPAA Training

1. All individuals, including volunteers and student observers, working in a unit designated as a Covered Component are required to complete training related to the regulatory obligations under the HIPAA Privacy and Security Rules.
2. PHI Partner Members are required to complete training on the safe handling of PHI and Personally Identifiable Information (PII).
3. Each Covered Component and PHI Partner Member will require individuals within their respective unit(s) to complete such training on a periodic basis, but in any event at least every four (4) years.
4. The University will provide faculty and staff training via an online training platform. Students will be provided with training through their individual colleges.

## F. Enforcement

1. Any employee, workforce member, student, or agent who violates this Policy shall be subject to appropriate disciplinary action.
2. Any other individual who violates this Policy shall be subject to appropriate corrective action, including, but not limited to, termination of their relationship with the University.

## IV. DEFINITIONS

- A. **“Business Associate”** means a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a Covered Component. A member of the Covered Component’s workforce is not a Business Associate.
- B. **“Covered Component”** means an area within a Hybrid Entity that would meet the definition of Covered Entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions (i.e., noncovered health care provider) or performs activities that would make the component a Business Associate of the entity if it were legally separate.
- C. **“Covered Entity”** is defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any Health Information in connection with transactions for which HHS has

adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. is a health care provider, health plan, or health care clearinghouse that transmits Health Information in electronic form in connection with a Covered Transaction.

- D. **“Covered Transaction”** means the transmission of information between two parties to carry out financial or administrative activities related to health care (e.g., health claims, payment, coordination of benefits, enrollment or disenrollment, eligibility for a health plan, and other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation 45 CFR § 160.103).
- E. **“Electronic Protected Health Information (“EPHI”)** means a form of PHI that is Individually Identifiable Health Information transmitted by electronic media or maintained in electronic media. Electronic Protected Health Information does not include education records or treatment records covered by the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) or employment records held by the University in its role as an employer.
- F. **“Health Information”** means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and that is related to the past, present or future physical or mental health condition of an individual, the provision of health care of an individual, or the past, present or future payment for the provision of healthcare to an individual.
- G. **“Hybrid Entity”** means a single legal entity (1) that is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates health care components.
- H. **“Individually Identifiable Health Information”** means any health information, as defined above, that identifies an individual or where there is reasonable basis to believe that the information can be used to identify an individual.
- I. **“PHI Partner Members”** are employees and others within the schools/departments/units University schools/departments/units that are not identified as a Covered Component but that encounter personal Health Information (PHI) in their job functions.
- J. **“Protected Health Information (“PHI”)** means Individually Identifiable Health Information that is collected from an individual, created or received by a health care provider, health plan, health care clearinghouse, or other employee of one of the Covered Components of the University. This PHI is confidential and must be treated as protected under HIPAA. Protected Health Information relates to the past, present, or future physical or mental health or condition of an individual;

the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

<b>Revision Effective Date</b>	<b>Purpose</b>