University of Colorado
Denver | Anschutz Medical Campus

**HIPAA Policy 9.1**

| | |
|---|---|
| **Title:** | **Security Management** |
| **Source:** | **Office of Information Technology** |
| **Prepared by:** | **Associate Vice Chancellor for the Office of Information Technology** |
| **Approved by:** | **Vice Chancellor for Research** |
| **Effective Date:** | **January 1, 2018** |
| **Replaces:** | **July 1, 2013** |
| **Applies:** | **University of Colorado Denver \| Anschutz** |

---

## Introduction

### *Purpose*

This security policy outlines minimum standards for ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) received, maintained or transmitted by all UNIVERSITY HIPAA Covered Components (outlined in APS #5055 – HIPAA Hybrid Entity Designation), as well as other offices which support these entities (listed below as "Support Services"). Covered Components shall meet or exceed these standards by implementing the necessary administrative, physical and technical safeguards as appropriate based on their assessments of risk. Compliance with these standards by the offices which support the Covered Components is limited to their activities that directly involve creation or receipt of ePHI in support of Covered Components and not activities related to services provided to non-covered areas of the UNIVERSITY.

### *HIPAA Reference*

45 C.F.R. §164.308(a)(1)(i); §164.308(a)(1)(ii)(A); §164.308(a)(1)(ii)(B); §164.308(a)(1)(ii)(D)

45 C.F.R. §164.308(a)(6)

45 C.F.R. §164.306(a); §164.306(e)

### *Applicability*

While application of this policy to any sensitive data is considered "best practice" and should be considered by all areas of the UNIVERSITY when storing or transmitting such information, it is only mandated for those areas the UNIVERSITY has designated as HIPAA "Covered Health Care Components" (Covered Components). In addition to the Covered Components, offices that

support such covered activities carried out by the Covered Components must also do so according to this policy.

Certain data is specifically excluded from coverage under HIPAA, most importantly:
(1) student records, except for student patient data (Family Educational Rights and Privacy Act (FERPA)) ;
(2) employment records, except for health benefits records; and
(3) information "de-identified" under HIPAA standards.

**Policy Statement**

The UNIVERSITY shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI and shall implement security measures sufficient to reduce risks and vulnerabilities. Such measures shall be implemented based on the level of risks, capabilities, and operating requirements of each office/department of the UNIVERSITY. These measures will include, as appropriate and reasonable, administrative, physical and technical safeguards, as defined in the Privacy Rule.