Table of Contents

Privacy and Security Policies and Procedures 1
Overview 1
Purpose 1
Applicable University-wide policies related the Data Privacy and Policies 1
University of Colorado IT Security Program Policy 1
University of Colorado Denver Security Management HIPPA Policy 2

Privacy and Security Policies and Procedures

1. University HIPAA Policy http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx

Overview

Data privacy is a critical component of the School of Education & Human Development (SEHD) operations. The protection and management of the various types of student, staff, faculty, and research subject Personally Identifiable Information (PII) is critical to the SEHD's operations. SEHD computer systems and related devices collect and record data as required for educational delivery, management, administration, reporting, assessment, and research purposes. This type of information is protected should never be disclosed to unauthorized individuals.

Purpose

This policy reiterates the SEHD's comitment to the general privacy requirements for information captured or generated by the SEHD's operations, systems, network devices, or communications as specified by University of Colorado system and the University of Colorado Denver.

Applicable University-wide policies related the Data Privacy and Policies

University of Colorado IT Security Program Policy

All data and information resources of the SEHD are subject to University of Colorado's IT Secuirty Program policy, APS-6005.

The goals of the University IT Security policy are as follows:

1. All members of the University community are aware of and are sufficiently trained to carry out their responsibilities for protecting University Infromation and IT Resources.
2. University information is regarded as a strategic organizational asset and is treated in a manner consistent with that of other strategic assets, such as financial and facility assets
3. IT Secuity is not considered a technical concern, but is addressed as a strategic business issue by integrating IT security safeguards into University business processes.
4. University resources are applied judiciously to IT security issues by focusing on those that represent the greatest risk to University operations and information.
5. IT security incidents are promptly detected and responded to in a manner that limits the impact to the security of University information and the operations of the University.

Please proceed to APS-6005 to learn how the university meets these goals.

University of Colorado Denver Security Management HIPPA Policy

As applicable, the most secure SEHD data are subject to the UCD Security Management HIPPA policy, HIPPA Policy 9.1.

Purpose of the UCD Security Management HIPPA policy:

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

Applicability of the UCD Security Management HIPPA policy

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.

From:
https://wiki.cu.studio/ - **SEHD Wiki**

Permanent link:
https://wiki.cu.studio/policy/data_privacy/privacy_and_security

Last update: **2019/05/20 17:22**