Table of Contents

Access Control

University of Colorado IT Security Program Policy

All data and information resources of the SEHD are subject to University of Colorado's IT Security Program policy, APS-6005. Within the policy it describes the requirement of minimum necessary access to data:

> Although students, faculty, and staff require access to University information resources for academic and business purposes, this access must be limited to what is needed for his/her work. Use of resources beyond that which is authorized results in unnecessary risks to University information with no corresponding academic or business value.

University of Colorado Denver HIPPA Policy

As applicable, the most secure SEHD data are subject to the UCD Workforce HIPPA policy 9.4. The policy describes what must be included in a unit's access control procedures.

> The UCD Information Technology Services Department (ITS) offers central disk storage and backup services which many departments and units use for maintaining their data. While central ITS systems meet the HIPAA physical security and contingency planning requirements, departments and units must still take care to address controls for workstation security, account management, and controlling access to ePHI they create or house.

Access to the SEHD Secure Data Server

Only appropriately identified, validated and authorized individuals will have access to the SEHD Secure Server.

To gain access a user must complete the following.

- The user completes and documents their completion of the required security trainings.
- The user reads and signs the SEHD Secure Data Server Access Agreement
- The user's supervisor or sponsor reads and signs the SEHD Secure Data Server Supervisor/Sponsor Agreement
- The user completes the SEHD Secure Data Server Access Form. The form will require that the user provides the minimum necessary data they will need to perform their task.

A data user's supervisor or sponsor will

- Re-evaluate access rights when a workforce member’s access requirements change and e-mail the Data Governance Manager if necessary to modify the user's access.
- Contact the Data Governance Manager in the event the data user's employment or affiliation with SEHD has ended.

The Data Governance Manager will

- Review the user's required trainings, SEHD Secure Data Server Access Agreement, SEHD Secure

Data Server Supervisor/Sponsor Agreement, and the SEHD Secure Data Server Access form.
- Grant, modify, or terminate the user's access to the SEHD Data Server.
- Send an e-mail with the decision to the data user, the data user's supervisor, SEHD HR, and SEHD IT.
- Remove the data user's access in the event the data user's employment or affiliation with SEHD has ended.
- Remove the data user's access in the event of a breach that endangers the security of the Data Server.
- On an annual basis review all user's that have access and modify or remove access as necessary.
- Maintain an auditable trail of requests, modification of access rights, and termination of access to the SEHD Secure Data Server.