

Table of Contents

Data Privacy Policies 1

Data Privacy Policies

1. [Privacy and Security Policies and Procedures](#)
2. [Identification of a Privacy and Security Board and Officer](#)
3. [Management Oversight of Privacy and Security Programs](#)
4. [Sanctions for Violations of Policies and Procedures](#)
5. [Reporting Potential Problems in Privacy and Security](#)
6. [Incident Response and Incident Response Mitigation](#)
7. [Privacy and Security Training](#)
8. [Access Control, Minimum Necessary Access and Verification for Access to Data User/SEHD Database Server/OIT](#)
 1. [APS-6005](https://www.cu.edu/ope/aps/6005)
 2. [University HIPAA Policy](http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx)
 3. [APS-6001](https://www.cu.edu/ope/aps/6001)
9. [Password Management User/SEHD Database Server/OIT – complying with university policy](#)
 1. [University Password Policy](http://www.ucdenver.edu/faculty_staff/employees/policies/Policies%20Library/Admin/fp5-13.pdf)
10. [Transmitting Sensitive Information Securely including Faxing and Email User/SEHD—duplicative with #1](#)
 1. [Email and Webmail Stay Secure](https://www1.ucdenver.edu/offices/office-of-information-technology/software/how-do-i-use/email-and-webmail)
 2. [HIPAA Policy 7.1 Safeguards](https://www1.ucdenver.edu/docs/default-source/offices-oit-documents/it-related-policies/hipaa-7-1-safeguards.pdf?sfvrsn=48bb7b8_6)
11. [Log-in Monitoring Database Server/OIT](#)
 1. Needs to be implemented and documented
 2. OIT has an internal standard for logging, monitoring and auditing that applies to all servers managed by CU Denver OIT.
 3. [HIPAA Policy 9.3 Auditing](http://www.ucdenver.edu/research/Research%20Administration%20Documents/9.3%20Auditing.pdf)
12. [Workstation Security Configuration User/SEHD, Server/OIT – duplicative with #1](#)
 1. [APS-6005](https://www.cu.edu/ope/aps/6005)
 2. [University HIPAA Policy](http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx)
13. [Device and Media Control Server/OIT – duplicative with #1](#)
 1. [APS-6005](https://www.cu.edu/ope/aps/6005)
 2. [University HIPAA Policy](http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx)
14. [Securing Materials with Data User/SEHD-duplicative with #1](#)
 1. [Security and Compliance Hard Drive Disposal](https://www1.ucdenver.edu/docs/default-source/offices-oit-documents/it-related-policies/hipaa-7-1-safeguards.pdf?sfvrsn=48bb7b8_6)
15. [Encryption Database Server/OIT](#)
 1. [Encrypt Your Laptop Guidance](https://www1.ucdenver.edu/offices/office-of-information-technology/software/secure-campus/encryption)
 2. [Guide to Secure Devices](https://www1.ucdenver.edu/offices/office-of-information-technology/software/secure-campus)

- [us/guide-to-secure-devices](#)
- 3. APS-6005 <https://www.cu.edu/ope/aps/6005>
- 4. University HIPAA Policy <http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx>
- 16. [Authorizations for Personal Health Information](#), if applicable User/SEHD -NA
 - 1. University HIPAA Policy <http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx>
- 17. [Permitted Uses and Disclosures of PHI](#), if applicable User/SEHD—NA
 - 1. University HIPAA Policy <http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx>
- 18. [HIPAA Status](#), if applicable Server/OIT
 - 1. UC Denver’s File servers are HIPAA compliant.
 - 2. Units/Departments can request assistance from the RAC team on the security of data usage.

<https://www1.ucdenver.edu/offices/office-of-information-technology/services/security-and-compliance>
- 19. Business Associate Status, if applicable
 - 1. NA
- 20. [Designating Sensitive Information](#) User/SEHD - may be duplicative
 - 1. University Data Classifications and Impact

<https://www.cu.edu/ois/data-classifications-impact>
- 21. [Risk Assessments and Management](#) User/SEHD - duplicative
 - 1. University HIPAA Policy <http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx>
- 22. [Change Control Procedures](#) User/SEHD - user access/retiring users
 - 1. OIT is also working on a process flow diagram to guide units/departments on their role in this process and how the OIT CAB process fits into the process.
- 23. [Audit and Evaluation Procedures](#) User/SEHD Server/OIT - designated liaison and form for auditors
 - 1. Units/Departments can request assistance from the RAC team on the security of data usage, but we are not auditors, nor do we have a specific form.

Sample Local Education Agency Policy Links:

<http://www.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies>

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

Permanent link:
https://wiki.cu.studio/policy/data_privacy?rev=1553800338

Last update: **2019/03/28 19:12**

