Table of Contents

Log-in Monitoring

University Internal Standard

OIT has an internal standard for logging, monitoring and auditing that applies to all servers managed by CU Denver OIT. Click her to view the version that was effective as of July 1, 2017. Please contact OIT's Risk and Compliance team for the most up to date version.

According to the standard the following details are logged and saved on a centralized logging server for at least six months:

1. Timestamp
2. Event, status, and/or error codes
3. Service/command/application name
4. User or system account associated with an event
5. Device used (e.g. source and destination IPs, terminal session ID, web browser, etc)

The events related to the following categories are logged:

1. Operating System(OS) Events
2. OS Audit Records
3. Application Account Information
4. Application Operations
5. File Access (files containing ePHI or Highly Confidential information)

University of Colorado Denver HIPPA Policy

As applicable, the most secure SEHD data are subject to the UCD Auditing HIPAA Policy 9.3. The auditing policy requires units that hold medium to high risk ePHI must create a Audit Control and review Plan. Within that plan it states:

> The system hardware, software, and applications must have the capability of creating log files. These logs must include, but are not limited to:

1. User ID;
2. Login date/time; and,
3. Activity time.

> Units must monitor login success and failure to systems that host ePHI. To ensure that unauthorized login attempts are discovered, discrepancies or unusual login patterns must be reported to the department administrator and HIPAA Security Officer.