Table of Contents

Workstation Security Configuration

Applicable University of Colorado Denver Policies

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. The policy states:

> Ordinarily, Highly Confidential informationshall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and adequately secured. If Highly Confidential informationis stored on a workstation or mobile computing device or transmitted to an external network or organization, IT resource usersshall encrypt or adequately protect that information from disclosure. If Confidential information is stored on a workstation or mobile computing device or transmitted to an external network or organization, IT resource users shall adequately protect that information from disclosure. In addition to encryption, adequate protections may include the use of passwords, automatic logoffs, and secure Internet transmissions.

University of Colorado Denver HIPPA Policy

The most secure SEHD data are subject to the UCD Workforce HIPPA policy. The policy states

> Computer workstations accessing ePHI must maintain security configurations that restrict access to ePHI to only those workforce members that have been legitimately granted access. Recommended security configurations include, but are not limited to:
>
> - enabling a password protected screen saver;
> - setting computers or applications to automatically terminate a computing session after a set period of idle time;
> - the use of campus standard anti-virus products; and
> - applying security patches to computer software applications and operating systems
>
> UCD ITS will disconnect workstations from the network that pose a threat to UCD information systems due to a suspected policy violation, workstation intrusions, virus infestations, and other conditions which might jeopardize UCD information or work.
>
> Workstations storing ePHI or that may be used to access ePHI must be located in areas with controlled access. An electronic audit trail of access must be maintained. It is the responsibility of unit administrators to establish and enforce a facility security plan to ensure access to workstations under their jurisdiction is restricted to authorized users.

SEHD Secure Data Server

Any workstation that has access to the SEHD Secure Data Server must meet the requirements of the UCD HIPPA Policy.