University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 7.1

Title:	**Safeguards – to Protect the Privacy of PHI**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**02/26/03**
Applies:	**All UCD campuses**

Introduction

Purpose

The UCD has the responsibility to maintain appropriate **administrative**, **technical**, and **physical** safeguards to keep protected health information (PHI) from any unauthorized use or disclosure, pursuant to HIPAA standards. Efforts to safeguard PHI are expected to be appropriate to the situation and reasonable in regard to effort and expense.

These policies have been developed in coordination with UCD departments and UCD Affiliates. Accountability for complying with HIPAA regulations applies to everyone in the UCD organization.

Reference

45 C.F.R. § 164.530(c)

Applicability

This HIPAA Policy applies to all PHI that exists in either electronic or paper form that is physically housed at the UCD Campus or otherwise managed under the direction of UCD organizational units or individuals.

Policy

The UCD HIPAA Privacy Officer and HIPAA Security Officer are responsible for drafting institutional policies for the UCD that are both appropriate and reasonable in regards to protecting the privacy of PHI.

Given that the UCD has an environment of distributed ownership and administration of electronic systems and paper records containing PHI, the direct responsibility of maintaining compliance with this policy resides with the organizational units and individuals owning and administering these systems.

Campus HIPAA Officers will serve as resources to campus units in the areas of maintaining campus-wide compliance data, coordinating HIPAA education efforts, and consulting with units to address remediation issues.

Penalties and disciplinary actions will arise from non-compliance with HIPAA policies, after appropriate HIPAA educational activities have taken place and if remediation of reoccurring issues has failed.

Procedures

Described below are UCD expectations in the areas of administrative, technical, and physical safeguards. HIPAA Regulations provide some specifics regarding what the Federal Government requires in the area of safeguarding PHI.

Administrative Safeguards

Individuals assigned the responsibility for developing, utilizing, or managing electronic systems or paper records containing PHI are responsible for registering with the UCD HIPAA Security Officer for the purpose of building an institutional PHI inventory.

Individuals and units handling PHI will be asked to complete surveys regarding HIPAA compliance. Completed survey records will be maintained by the HIPAA Security Officer.

Organizational units or individuals administratively responsible for handling PHI are expected to keep their processes and practices in compliance with UCD HIPAA policies.

Contact information for the UCD HIPAA Privacy Officer and HIPAA Security Officer can be found at http://www.ucdenver.edu/hipaa/contacts.htm for self-reporting of non-compliance issues. The UCD HIPAA Privacy Officer and HIPAA Security Officer will assist system owners with self-assessments, reviewing issues brought to their attention regarding non-compliance, and assist where possible with remediation efforts.

All University systems and equipment are subject to compliance inspections. Spot audits will be performed to verify self-assessment reports.

Owners of the electronic and paper systems containing PHI bear the responsibility for any labor or expenses associated with bringing their systems and processes into compliance.

Technical Safeguards

Technical aspects associated with ensuring the privacy of PHI will in some cases require the expertise of information technology professionals. In those situations, responsibility for ensuring the privacy of PHI will be shared jointly by the system administrator and end user.

1. End User Responsibilities

    a. Account Access

    Every individual shall have a personal login and password for authorization and authentication before accessing PHI except where specifically approved due to unique circumstances. Each request for an exception will be reviewed by the HIPAA Security Officer on a case-by-case basis. Logins and passwords shall not be shared and group logins will not be issued, except in special circumstances. Requests for these accounts will also be reviewed on a case-by-case basis.

    The use of hardened passwords is required, when feasible, on all systems containing PHI. Methods for hardening passwords and other password policy information is contained on the UCD ITS web site.

    Users should log out of or "lock" their computer systems when not in use to reduce the risk of improper access to PHI.

    b. Desktop Computers

    PHI should not be stored on the hard drive of desktop computers. It is easier to physically protect a limited number of servers than to protect every end user's desktop. Placing PHI on the hard drive of a desktop computer raises the security requirements for that desktop to the level of a server containing PHI.

    Screen savers should be enabled and password protected so that screen displays are masked after a period of inactivity and to ensure that a password is required before the display can be reactivated. If use of a shared computer is required, each end user should log off the system prior to relinquishing the computer to the next user.

    Individuals operating computers on the UCD campus network have a responsibility to operate and maintain current anti-virus software. Security patches for software and operating systems shall also be maintained.

c. E-Mail

If PHI must be transmitted via e-mail, and the e-mail recipient is part of the internal e-mail system, i.e. UCD, UCH, CHC, or UPI, the e-mail does not need to be encrypted, given that the network is private. If the e-mail must be sent across the Internet to either a patient or another entity covered by HIPAA, encryption should be applied to the e-mail message. Personal e-mail accounts (ex. AOL, yahoo) may not be used to transmit e-mail containing PHI, due to the fact that these e-mail systems are not encrypted.

d. Remote Access

Individuals accessing UCD via remote access have a responsibility to operate and maintain current anti-virus software at their remote locations. Software security patches shall also be maintained. Users of DSL or cable modem services are required to operate virtual private network (VPN) software and personal firewall software in addition to anti-virus software to mitigate the increased risks posed by these high-speed connections. The UCD ITS Department reserves the right to verify that protections are in place.

e. Portable Computing Devices

Portable computing devices include a range of electronic devices such as (but not limited to): laptops, thumb drives, cell phones, and tablet computers. Given their small size and portability, loss or theft is a constant possibility.

The best practice is to keep sensitive information off such devices entirely. Failing that, devices should be password protected and, where possible, the PHI data on the devices encrypted. Physical security is critical -- end users and departments are responsible for keeping track of PDAs, laptops, and other mobile devices.

If the portable computing device is lost or stolen, the user of that system is responsible for notifying his or her department and the UCD HIPAA Privacy Officer.

2. System Administrator Responsibilities

The UCD ITS Department will periodically scan systems to ensure that safeguards are in place.

The UCD ITS Department will notify the UCD HIPAA Security Officer immediately if it finds that a system does not have the appropriate safeguards.

a. Access Controls

Access to systems containing PHI shall only be granted after an account creation process has been completed. Components of an account creation process must include positive identification of the individual, determination of the person's roles and access requirements, education of the individual regarding proper use of the account, and written acceptance of University and unit level policies regarding appropriate use of the resources. Where feasible, access to the PHI will be limited to the individual who requires this access and only to the extent minimally necessary to fulfill that person's work obligations.

b. Audit Trails

Audit trails can be used to trace suspicious patterns of use and as a backup to the limitations that access controls provide. Where computer system capabilities allow it, audit trails to activities performed on a system, such as user logins, logouts, and accesses to PHI, should be created. System administrators shall review audit records on a routine basis.

c. Change Control Management

The processes by which database systems and software applications are developed and changed should be given specific attention. Reasonable and appropriate methods will vary based on the nature of the data and the type of system involved. For example, programming changes in an electronic medical record system should have more change controls in place than would be expected for the updating of a computer spreadsheet.

3. Wired and wireless Networks

Wireless network devices use radio frequency transmissions to replace wire connections. Signals broadcast by wireless devices can travel far beyond the confines of any structure, and so must be protected in other ways.

UCD Information Systems is the only approved provider of wireless networking on the UCD campus. UCD ITS ensures that wireless network signals are encrypted, thereby reducing the vulnerability of wireless eavesdropping and the improper disclosure of PHI.

4. Providing Internet Access to PHI

Since the Internet is inherently insecure and there is a risk of data being intercepted, PHI shall not be transmitted over the Internet, including Internet e-mail, unless the data is encrypted. Industry-accepted methods of encrypting Internet traffic include, but are not limited to, secure sockets layer (SSL) encryption, virtual private networking (VPN), secure Citrix software, and secure shell (SSH).

5. Fax Machines

Fax machines used for transmitting or receiving PHI must be in locations secured from the general public. Before sending out faxes, ensure that the destination phone number is correct and include appropriate cautions and disclaimers on the fax cover sheet. Faxes should always have cover sheets.

Physical Safeguards

It is natural to focus on technical aspects of security, but physical protections are critical too. Owners of systems containing PHI shall at a minimum address the following physical safeguards:

• All paper PHI records must be kept in a locked file in a locked room (eg. Two physical barriers).

• Restrict access to areas with printed materials, fax machines, or computers containing PHI.

• All UCD owned laptops must be encrypted.

• When no longer needed, ensure that any printed material is shredded and portable storage devices containing PHI are properly erased or destroyed.

Neglect of physical security leads to security problems. Even the most sophisticated electronic security efforts can be defeated by inattention to the basics of physical security.