

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.1 Security Management	Latest Revision: 03/31/05 Page: 1 of 5
---------	----------------------------	---

I. Purpose, Reference, and Responsibility

A. Purpose

The purpose of this policy is to outline the procedures for secure management of ePHI, including risk analysis and management, and security management, evaluation and maintenance.

B. Reference

45 C.F.R. § 164.308(a)(1)(i) & (ii)(A) & (B).
45 C.F.R. § 164.308(a)(8).
45 C.F.R. § 164.306(e).

C. Responsibility

It is the responsibility of anyone at UCDHSC who uses, discloses or maintains ePHI to practice security management. This includes faculty, staff, students, trainees, volunteers, etc. The UCDHSC HIPAA Security Officer is responsible for overall periodic campus risk analyses, compliance program evaluations, and maintenance.

II. Applicability and Definitions

A. Applicability

This policy is applicable to all units of UCDHSC that create, receive, maintain or transmit ePHI, including faculty, staff, students, trainees, volunteers, etc.,

B. Definitions

Availability
Computer Tracking Worksheet
Confidentiality
Electronic Protected Health Information (ePHI)
Information Systems Department (IS)

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.1 Security Management	Latest Revision: 03/31/05 Page: 2 of 5
---------	----------------------------	---

Integrity
Security Rule
Workforce

III. Policy

A. Security Management Process

1. All members of the UCDHSC workforce who create, receive, maintain or transmit ePHI must implement policies and procedures to prevent, detect, contain, and correct security violations. See the Incident Response policy (<http://www.uchsc.edu/hipaa/internal/docs/p.2.pdf>) for details on reporting suspected security violations.

B. Risk Analysis

1. Units and members of the UCDHSC workforce who maintain ePHI must conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks and vulnerabilities must be assessed equally to ePHI that is in transit or at rest. The analysis should attempt to identify all relevant losses that could be anticipated if security measures were not in place. Units or workforce members who maintain ePHI may use the computer tracking worksheet to assist in conducting risk analyses. This worksheet is available on the IS website at: <http://www.uchsc.edu/is/security/>.
2. Unit-level risk analyses should be conducted every two (2) years or as needed based on significant environmental or operational changes to the unit security of ePHI. For example, a risk analysis should be conducted prior to implementing a new web-based application that will contain ePHI.
3. The UCDHSC HIPAA Security Officer is responsible for conducting a campus-wide risk analysis and for retaining documentation of the risk analysis. The HIPAA Security Officer will conduct a campus-

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy: 9.1
Security Management

Latest Revision: 03/31/05
Page: 3 of 5

wide risk analysis as needed in response to significant environmental or operational changes to the campus-wide security environment, but under no circumstances, no less than every two (2) years, beginning April 2005.

4. At a minimum, risk analysis documentation should identify the potential risks and vulnerabilities to the confidentiality, integrity or availability of ePHI.

C. Risk Management

1. The decentralized nature of UCDHSC necessitates that units and members of the UCDHSC workforce who create, receive, maintain or transmit ePHI must implement security measures sufficient to reduce unit-level risks and vulnerabilities to ePHI confidentiality, integrity, and availability to a reasonable and appropriate level. The risk management decisions must be based on the required risk analysis above.
2. Risks can be accepted, transferred, mitigated or avoided. Units and members of the UCDHSC workforce who create, receive, maintain or transmit ePHI may follow the risk management graph below in determining what actions should be taken with identified risks.

High Value of Data X Low Risk = Mitigate	High Value of Data X High Risk = Avoid or Mitigate
Low Value of Data X Low Risk = Accept	Low Value of Data X High Risk = Accept

3. Units or members of the UCDHSC workforce must create a risk management plan that addresses all reasonably anticipated threats or hazards to the security or integrity of ePHI. This plan must be submitted to and approved by the UCDHSC HIPAA Security Officer. After approval, units must implement and follow their risk management plans.

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.1 Security Management	Latest Revision: 03/31/05 Page: 4 of 5
---------	----------------------------	---

4. All decision-making practices, implementation of analysis findings, and policies and procedures adopted must be documented and provided to the UCDHSC HIPAA Security Officer.
5. EPHI must be protected against any reasonably anticipated inappropriate uses or disclosures pursuant to the UCDHSC HIPAA Privacy Policies.
6. The UCDHSC HIPAA Security Officer shall work in conjunction with IS to create a risk management plan at a campus level.
7. It is the responsibility of anyone at UCDHSC who creates, receives, maintains, or transmits ePHI to practice security management, which includes risk management. All violations of this policy are subject to the Sanctions Policy:
<http://www.uchsc.edu/hipaa/internal/docs/1.5.doc>

D. Maintenance

1. Unit security measures must be reviewed and modified by units as needed to continue provision of reasonable and appropriate protection of ePHI. These measures must be reviewed on at least an annual basis.
2. All unit reviews and any modifications of security measures must be documented and provided to the UCDHSC HIPAA Security Officer.
3. The UCDHSC HIPAA Security Officer will perform a campus-level security measure review at least annually and will modify any campus-level security measures as needed.

E. Evaluation

1. All security policies and procedures adopted by UCDHSC at either a campus-wide or unit-level must be periodically evaluated to assure continued viability in light of technological, environmental, or operational changes that could affect the security of ePHI.

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.1 Security Management	Latest Revision: 03/31/05 Page: 5 of 5
---------	----------------------------	---

2. Units with ePHI are responsible for evaluating their unit-level policies and procedures and upgrading their policies and procedures if needed. Units must evaluate their unit-level policies and procedures as needed, in response to significant environmental or operational changes to their environment, but under no circumstances no less than every two (2) years.
3. Working with the individual units, the UCDHSC HIPAA Security Officer shall perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of ePHI. This evaluation must establish the extent to which UCDHSC security policies and procedures meet the requirements of the Security Rule. This evaluation must be performed no less than every two (2) years and in response to significant environmental or operational changes to the security of ePHI at a campus-level. The UCDHSC HIPAA Security Officer must immediately perform an evaluation if changes are made to the HIPAA Security or Privacy regulations or new federal or state laws are implemented that affect the privacy or security of ePHI.
4. All evaluations and upgrades must be documented and sent to the UCDHSC HIPAA Security Officer.

F. Documentation

1. All documentation pursuant to this policy must be kept for a period of at least six (6) years from the date of creation of the document or the date when the document was last in effect, whichever is later.
2. Documentation pursuant to this policy (including risk analysis documentation) must be stored securely.