Introduction

Purpose
This policy outlines the procedures for secure management of electronic Protected Health Information (ePHI), including risk analysis and management, and security management, evaluation and maintenance.

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)

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

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

Procedures

Security Management Process

All members of the UCD workforce who create, receive, maintain or transmit ePHI must implement policies and procedures to prevent, detect, contain, and correct security violations.

A. Risk Analysis

1. Units and members of the UCD 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.

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. Examples of such changes include: significant security incidents, significant changes to the organizational or technical infrastructure, hardware and software upgrades, and changes to information security requirements or responsibilities that impact ePHI.

3. The UCD 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-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.

5. All BAAs and DUAs must include a Data Management and Security Plan, approved by the UCD Security Officer, prior to submitting to ORC for signature.

B. Risk Management
1. The decentralized nature of UCD necessitates that units and members of the UCD 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 UCD 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.

<table>
<thead>
<tr>
<th>High Value of Data X</th>
<th>Low Risk = Mitigate</th>
<th>High Value of Data X</th>
<th>High Risk = Avoid or Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Value of Data X</td>
<td>Low Risk = Accept</td>
<td>Low Value of Data X</td>
<td>Low Risk = Accept</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Units or members of the UCD 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 UCD HIPAA Security Officer. After approval, units must implement and follow their risk management plans.

4. All decision-making practices, implementation of analysis findings, and policies and procedures adopted must be documented and provided to the UCD HIPAA Security Officer.

5. EPHI must be protected against any reasonably anticipated inappropriate uses or disclosures pursuant to the UCD HIPAA Privacy Policies.

6. The UCD HIPAA Security Officer shall work in conjunction with Information Technology Systems (ITS) to create a risk management plan at a campus level.

7. It is the responsibility of anyone at UCD 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.

C. 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 UCD HIPAA Security Officer.
3. The UCD HIPAA Security Officer will perform a campus-level security measure review at least annually and will modify any campus-level security measures as needed.

D. Evaluation

1. All security policies and procedures adopted by UCD 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.

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 UCD 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 UCD 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 UCD 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 UCD HIPAA Security Officer.

E. 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.