HIPAA Policy 9.1 – Security Management
PROCEDURES

OBJECTIVE

The HIPAA Security Standards require Covered Entities, or a Hybrid Entity's Covered Components to:

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." and, engage in risk management to, "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply."

Compliance with the HIPAA Security Standards involves the following:

A. Initial Compliance Plan

The following steps should be followed by HIPAA Units (defined in HIPAA as "Health Care Components") when conducting the Risk Analysis, appropriately documenting each:

1. Consider the location and access of ePHI and review pertinent university HIPAA policies to determine what should be considered in the scope of the Risk Analysis.

2. Identify potential threats to the confidentiality, integrity and availability (access) to the ePHI.

3. Evaluate the likelihood and impact related to the threats identified.

4. Identify one or more potential actions to be taken for each that shall be intended to mitigate the risk. Such actions may be adjusted over time based on reasonableness and/or operational implications of each. Note: there may be multiple options for mitigating a risk with differing costs and/or levels of impact.

5. Engage with appropriate stakeholders to determine which action(s) will be taken to mitigate each risk.

6. Develop and document a plan for implementing the mitigation actions.

B. On-Going Risk Management

The On-Going Risk Management program will require the following steps be taken on a scheduled basis:

1. Identify new risks. Add any such risks to the Initial Risk Assessment following the same process as outlined in the Initial Risk Assessment above.

2. Review previously identified/existing risks. Determine if any risk has changed in nature or is no longer a risk. Make adjustments to the Initial Risk Assessment as appropriate.

3. Update the status of all risks.

4. When appropriate, document plan for addressing new identified risks.

5. Provide an updated Risk Assessment to the stakeholders for their review and feedback, as appropriate.

C. 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.

Related HIPAA Documents

HIPAA Risk Analysis
The university's OIT Risk and Compliance (RAC) team has developed a program to assist units meet their compliance to the HIPAA Security Rule. Resources for this program can be located at: http://www.ucdenver.edu/SecureCampus/

Contact for Questions Related to this Policy
University Chief Information Security Officer
UCD-OIT-RAC@ucdenver.edu