Office of Information Technology
UNIVERSITY OF COLORADO
DENVER | ANSCHUTZ MEDICAL CAMPUS

HIPAA Risk Analysis

Unit Compliance to the HIPAA Security Rule

OIT Security Risk and Compliance

PURPOSE

The purpose of this document is to provide guidance for units on how to perform a Risk Analysis of their environment as required in University HIPAA Policy 9.1.

Version 1.3

Contents

Executive Summary

The purpose of this document is to give guidance to departments, schools, offices and other campus units on the Anschutz Medical Campus, and to a much lesser extent CU Denver campus, in their responsibilities to meet compliance to the HIPAA Security Rule. In order to meet compliance, a Risk Analysis must be performed every two (2) years, or as needed based on significant environmental or operational changes to the unit security, in order to identify and address risks to University ePHI. This document will provide guidance on the Risk Analysis process. This document will provide guidance on the Risk Analysis process.

The audience for this document are holders (owners and custodians) of ePHI at the university. These owners and custodians of ePHI are responsible for the privacy and proper handling of ePHI and must meet the requirements of HIPAA compliance.

For additional information regarding University HIPAA policy refer to Appendix A.

CIA (Confidentiality, Integrity, and Availability)

The CIA triad is a widely-used security model that stands for Confidentiality, Integrity, and Availability. These key principles must be assured in any secure HIPAA system and a breach of any of the three can mean serious consequences to the University. The CIA triad is a model that is referred to and considered throughout the Risk Analysis process.

Confidentiality- Ensuring that the data only reaches the people it was intended for or authorized to view it.

Integrity- Assurance that the data has not changed and is trusted and accurate.

Availability- A guarantee that the data will be readily available to authorized people at all times.

The Unit should determine which principle is most important to them when performing a Risk Analysis of their HIPAA environment.

Unit Risk Analysis

The Risk Analysis Process

The steps below are a very generic description of the Risk Assessment/Analysis process and are meant as a good starting point. Follow all steps and document as you go through the process.

Start Here- Determining Scope and Gathering Data

1. Determine the scope of the analysis/assessment.
   - In a technical risk assessment, the scope should include any people, systems, applications, services, or facilities that are used in the process of receiving, storing, maintaining, and/or transmitting ePHI within your environment.
2. Gather data
   - Begin Steps 1 and 2 by completing the Scoping Questionnaire below. You cannot protect your ePHI without knowing who accesses your data, the type of data being protected, where the data stored, etc. The questionnaire will assist you with gathering the data required to begin the Risk Analysis.

Scoping Questionnaire

Unit:

Author (person filling out this form):

Author Email:

Author Phone:

Author Job Title:

Date:

What type of data is received, stored, maintained, and/or transmitted?

How does the data fit into the CU Data Classification model?
http://www.cu.edu/ois/data-classifications-impact

How will the data be used?

Where will the data be stored? Will it be stored on premise or off premise? If on premise, how will it be secured?

Who is responsible for the data?

How many records will be processed/stored?

Who will have access to the data? (CU staff/faculty only? Affiliates? Vendors?)

Where will the data be accessible from? (Only on campus? Off campus?)

Will you have Third party vendors that will host hardware, software, and/or infrastructure for this environment?

How do you Protect the data?

- OIT resources: (Email, File Server, Sharepoint, etc.)
- Third-party resources
- In-house Developed Resources

Remaining Steps in the Risk Assessment Process

3. Identify and document potential threats and vulnerabilities.
    - Following the data gathering step in the Risk Analysis process, you must identify your potential threats and where you feel your unit is vulnerable to a breach. Document your findings.
4. Assess current security controls.
    - What security controls currently in place will provide protection against the identified threats? Are there gaps where the control does not adequately protect the data?
5. Determine the likelihood of threat occurrence.
    - How likely is a particular threat to the data? Go through each identified threat and determine the likelihood of the threat occurring.
    - See Appendix A for a chart that will assist in determining likelihood and the Risk Score.
6. Determine the potential impact of threat occurrence.
    - If a particular threat occurs, how will it impact the unit? Will business continue? Will there be significant loss of data?
    - Refer to the University Data Classifications and Impact Page to assist you in determining the impact to your unit. http://www.cu.edu/ois/data-classifications-impact
    - See Appendix A for a chart that will assist in determining risk and the Risk Score.
7. Identify security controls
    - Determine what additional security controls must be put in place to remediate vulnerabilities.
8. Draft a Security Plan
    - Determine and document a Security Plan to address threats and vulnerabilities discovered during the Risk Analysis. The plan should explain how you will implement the controls in order to protect the data.
9. Implement the controls listed in the Security Plan
    - Implement controls and assess to ensure the data is secure.
10. Document the Implementation Plan
    - Document the plan for implementing each control listed in the Security Plan
11. Review every two years
    - The Security Plan is for the current state of your environment and should be reviewed every two years or as changes to the mission, changes in risk and changes in the environment occur.

Contact Us

The Risk and Compliance Team is here to help you if you need assistance. Please email us at UCD-OIT-RAC@ucdenver.edu or call the Help Desk at 303-724-4357.

Appendix A- Determining Likelihood and Impact of Threats

		Risk Score		
Likelihood	3	3	6	9
	2	2	4	6
	1	1	2	3
Risk Score = Likelihood X Severity		1	2	3
		Severity/Impact Level		

Impact	Rating	Likelihood
Low Impact: Limited adverse effect. The organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. Minor harm to individuals, minor financial loss, minor damage to organizational assets. Little potential for loss.	1	**Low Likelihood:** Unlikely the threat would occur.
Moderate Impact: Serious adverse effect. Significant degradation in mission capability for a duration of time and to the extent the organization's ability to perform its primary functions is significantly reduced. Results in significant remediation cost.	2	**Moderate Likelihood:** Likely the threat could occur.

High Impact: Severe or catastrophic adverse effect. Severe degradation or loss in mission capability for a duration of time and to the extent the organization is not able to perform its primary functions. Major financial loss, severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.	3	**High Likelihood:** High probability of the threat occurring. It is only a matter of time.

Appendix B- Relevant Documents and Web Pages

HIPAA Policy Documents:

http://www.ucdenver.edu/research/ORC/HIPAA/Pages/policies.aspx

HIPAA Policy 9.1 discusses Risk Analysis and Management requirements:

http://www.ucdenver.edu/research/Research%20Administration%20Documents/9.1%20Security%20Management.pdf

University Data Classifications and Impact Page:

http://www.cu.edu/ois/data-classifications-impact

NIST 800-30:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST 800-66:

http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Updates to 800-66: http://csrc.nist.gov/news_events/HIPAA-Jan2008_workshop/presentations/NIST800_66Update.pdf

Health and Human Services Risk Analysis Guidance:

Guidance on HIPAA Risk Analysis Requirements under the HIPAA Security Rule:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Basics of HIPAA Risk Analysis and Risk Management:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf