General Information

Policy Name:	HIPAA Risk Analysis & Risk Management
Category:	Risk Management – Corporate Compliance
Applies To:	All individuals who analyze and manage the risks to ePHI within Crouse Hospital.
Key Words:	HIPAA Security, Risk Management Risk Analysis, Security Management
Associated Forms & Policies:	HIPAA Risk Analysis Form (Doc #7840)
Original Effective Date:	03/01/12
Review Dates:	01/08/20, 01/10/22, 01/10/23, 01/08/24, 01/08/26
Revision Dates:	01/25/16, 01/12/18, 01/09/25
This Version's Effective Date:	01/09/25

Policy

It is the responsibility of Crouse Hospital to implement Risk Analysis and Risk Management policies & procedures to identify and prioritize the risks to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). Failure to do so could result in a potential disclosure or breaches of ePHI that would otherwise have been caught through the Risk Management/Analysis process. This policy in required by both HIPAA Security and New York State Cybersecurity standards.

Risk Analysis

Crouse Hospital is required to implement a Risk Analysis policy to review any and all potential threats and vulnerabilities that might affect the security of ePHI. A formal risk analysis should be performed for the following, but not limited to:

- New software, hardware, equipment, etc. that will have access to ePHI
- Updates to software, hardware, equipment, etc. that changes current access parameters to ePHI
- A potential disclosure or breach is discovered
- A potential flaw in current software, hardware, etc. is discovered
- A new State or Federal regulation, law, or guideline is introduced

If at any time a potential threat or vulnerability could impact the Hospital and gain access to ePHI, a risk analysis should be performed beforehand to prevent a security incident. Crouse Hospital's risk analysis process will include the following:

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine likelihood of threat occurrence
6. Determine potential impact of threat occurrence

7. Determine the level of risk
8. Identify all possible security measures
9. Engage key stake holders
10. Finalize documentation

Anyone who performs a HIPAA risk analysis should use HIPAA Risk Analysis Form (Doc #7840) to properly document the HIPAA risk analysis process.

Risk Management

Crouse Hospital is required to implement a Risk Management Policy to manage any and all risks that may affect the security of ePHI. A Risk Management procedure will be followed on a regular basis to ensure appropriate safeguards and measures are implemented to protect Crouse Hospital ePHI. The Risk Management procedure will include the following:

1. Review Risk Analysis
2. Create an action plan for implementing security measures
3. Implement security measures
4. Assign responsibilities accordingly
5. Evaluate and maintain security measures

Procedure

Risk Analysis

1. Identify the scope of the analysis

Crouse Hospital will identify the scope of the analysis by providing the following information:

- Identify the entity being analyzed
- Identify objectives for analysis
- Identify boundaries of the analysis

2. Gather data

The individual(s) conducting the risk analysis will gather information on Hospital ePHI. It may be impossible or impractical to gather all necessary data; the individual(s) conducting the risk analysis have the responsibility to get as much data as needed to create a thorough and complete analysis. It is the individual(s) discretion to determine when an acceptable amount of data is gathered.

3. Identify and document potential threats and vulnerabilities

The reviewer will identify all potential threats and vulnerabilities to ePHI. At this point, if a potential threat or vulnerability that is initially discovered is an exceptionally dangerous risk, Crouse Hospital reserves the right to temporarily stop and/or end the current risk analysis and deem the entity (i.e. a new application being reviewed for purchase) disqualified as an excessive risk.

4. Assess current security measures

Once all threats and vulnerabilities have been identified, current security measures will be reviewed. This may include, but not be limited to:

- Security software, hardware, network, and personnel

- Physical/environmental security measures
- Policies and procedures
- City, County, State, and Federal regulations

Only security measures currently in place will be subject for review. New or updated security measures will be disregarded unless they are currently being implemented as the analysis is being performed. Future regulations from Government agencies may be considered in the risk analysis on a case-by-case basis, depending on the impact it will have on the current risk analysis.

5. Determine the likelihood of a threat occurrence

Crouse Hospital will review all threats posed to the hospital and determine the likelihood that an identified threat may occur. The determination will be made with the following ratings:

- Low Likelihood – The odds of a threat occurring are low enough that any safety measures in place are sufficient enough or it is an acceptable low occurrence that safety measures are not necessarily needed at this time.
- Medium Likelihood – The odds of a threat occurring are enough that current safety measures may not be sufficient. Crouse Hospital should review ways to lower the likelihood whenever possible, as the odds of a threat occurring are large enough to warrant action.
- High Likelihood – The odds of a threat occurring will trigger a vulnerability. Crouse Hospital will be required to review the potential vulnerabilities to determine whether or not there are sufficient security measures in place to protect the Hospital.

The individual performing the risk analysis will make the best determination based on information within the analysis.

6. Determine the potential impact of a threat occurrence

Crouse Hospital will review the potential impact of a threat occurrence on all possible threats. The impact of a threat occurrence includes, but is not limited to:

- Unauthorized access to ePHI
- Temporary or permanent loss to ePHI
- Potential downtime from accessing ePHI

The determination will be made with the following ratings:

- Low Impact – The impact can either be minimal enough to not be an issue or be an acceptable occurrence that would not disrupt the security of Crouse Hospital.
- Medium Impact – The impact may be a substantial issue for Crouse Hospital. While the impact may not be critical or detrimental to the hospital, steps may need to be taken in order to mitigate this possible impact from occurring as it may cause potential disruptions in workflow or day-to-day operations as well as have an impact on security.
- High Impact – The impact represents a critical need for Crouse Hospital to prevent such an impact from occurring. This type of impact may affect Crouse Hospital's ability to function securely (or at all) and should be handled as a top priority.

The impact of a threat can vary depending on the situation, facility, personnel, outside parameters, etc. and as such all aspects should be considering when determining the impact of a threat occurrence. The individual performing the risk analysis will make the best determination based on the evidence at hand.

7. Determine the level of risk

During a risk analysis, the level of risk will be determined by comparing the following:

- The likelihood of a threat occurrence
- The impact of a threat occurrence

Keep in mind that there is no perfect equation to determine whether or not each vulnerability and threat is a risk to Crouse Hospital. The risk analysis is to gather as much data as possible on both the product/service and Crouse Hospital for the individual performing the risk analysis to make that determination. Different circumstances can yield different results. Review the "HIPAA Risk Matrix" within this policy to help determine the levels of risk.

The level of risk will be determined by following ratings:

- Low Risk: The risk is small enough where current security measures are sufficient to protect ePHI.
- Medium Risk: The risk is enough for Crouse Hospital to implement new and/or improve current security measures. While the risk may not need an immediate action or response, the Hospital should work towards mitigating them in an efficient and secure manner.
- High Risk: The risk is large enough for Crouse Hospital to formulate an action plan and mitigate the risk in a timely manner. Failure to do so could leave ePHI at risk of being compromised, stolen, deleted, etc.
- Critical Risk: The risk requires immediate and decisive action. Any delays could place the confidentiality, integrity, and availability of Crouse Hospital ePHI at serious risk.

No risk should be completely ignored and all risks should be documented for review and record-keeping purposes. All information for the analysis should be documented in the form "7840 HIPAA Risk Analysis Form" to determine whether the likelihood is Low, Medium, or High in regards to Crouse Hospital HIPAA Security.

8. Identify all possible security measures

Once all risk factors have been determined, Crouse Hospital will identify all possible and practical security measures that need to be in place for the final determination. This will help determine whether or not each risk can be mitigated properly and securely. Security measures can be, but are not limited to:

- New/Updated software, hardware, network, personnel, etc.
- New/Updated employee education, reminders, events, etc.
- New/Updated policies, procedures, protocols, forms, etc.

It is the responsibility of Crouse Hospital to determine all possible security measures to help mitigate any potential risks to Crouse Hospital ePHI. Failure to do so could put patient data at risk.

9. Engage the stake holders

Once all risks and possible security measures have been reviewed and documented, the individual(s) should engage the stake holders who will be directly affected by this risk analysis. This will help them understand the different risks associated with in their respective departments as well as ensure those impacted by the risk analysis are informed of any and all changes/updates that may occur. Crouse Hospital ePHI is used by many different departments and as such the individual(s) performing the risk analysis have the responsibility to inform the stake holders so they may be aware of any ePHI security threats.

10. Finalize documentation

The individual(s) performing the risk analysis will finalize documentation and present the analysis to the appropriate parties and channels. Any disputes or changes will be made by the individual(s) who performed the risk analysis and re-submitted until all parties and channels come to an agreement on the analysis. All finalized risk analysis documentation will be held for a period of six years.

Risk Management

1. **Review risk analysis**

   Review the HIPAA Risk Analysis that was performed. Ensure that all information is correct and indicates all potential solutions as well as security measures to reduce the risk to Hospital ePHI.

2. **Create an action plan for implementing security measures**

   An action plan should indicate the scope of the plan, the security measures being implemented; assign responsibility to those implementing the security measures and the timeframe to complete the plan. This ensures that risk mitigation is being performed, those responsible for the risk mitigation are documented, and a timeframe to notify the Hospital when the risk mitigation process will be complete.

   Action plans are working documents and may need to be updated. For example, if the timeframe is unable to be met due to constraints, the action plan should be updated accordingly. This will help Crouse Hospital understand any issues that develop as well as better planning for the implementation process for future security measures.

3. **Implement security measures**

   Crouse Hospital will implement the appropriate security measures to minimize the risk towards ePHI. A cost-benefit analysis may be performed as limited time, revenue, and resources may affect which security measures can be implemented. Crouse Hospital should review any and all information to determine the best course of action to protect Hospital ePHI.

4. **Assign responsibilities accordingly**

   Once the security measures have been implemented, it may be necessary to have an individual or even department continue to monitor and/or utilize the measures. Ensure the responsibilities are given to the appropriate entities. Any changes to the assigned responsibility should be documented to prevent possible confusion.

5. **Evaluate and maintain security measures**

   Evaluating and maintaining current security measures is paramount to protecting ePHI. Crouse Hospital should perform a number of actions in order to ensure that the security measures are acceptable. They include, but are not limited to:

   - Test current security measures for any possible gaps
   - Review any documented security issue findings on a regular basis
   - Ensure vendor support (if applicable) is continuous and up-to-date
   - Utilize surveys to determine possible gaps from employees
   - Continuously review new requirements to ensure security measures are meeting HIPAA Security requirements
   - Research new/better ways to protect ePHI from possible risks

References

HIPAA Security Rule 45 CFR 164§.308(a)(1)(ii)(A) – Risk Analysis

HIPAA Security Rule 45 CFR 164§.308(a)(1)(ii)(B) – Risk Management

HIPAA Security Rule 45 CFR § 164.316 – Policies and procedures and documentation requirements

CMS Minimum Security Requirements – Acceptable Risk Safeguards

New York State DoFS 23 NYCRR 500

Definitions

electronic Protected Health Information (ePHI): Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

Risk: A measure of the impact of something undesirable happening and its likelihood of occurring.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Threat: The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Addendums, Diagrams & Illustrations

See Next Page

I. Risk Analysis Matrix