General Information

Policy Name:	HIPAA: Responsibility, Evaluation, P&P, and Documentation
Category:	Risk Management – Corporate Compliance
Applies To:	Individual designated as the HIPAA Security Officer
Key Words:	HIPAA Security Officer, HSO, HIPAA Security
Associated Forms & Policies:	
Original Effective Date:	03/01/12
Review Dates:	01/29/16, 03/29/20, 03/25/22, 04/04/23, 04/12/24
Revision Dates:	05/29/25
This Version's Effective Date:	05/29/25

Policy

General

HIPAA (Health Insurance Portability and Accountability Act) Security requires certain elements to be conducted and carried out by Crouse. First and foremost, HIPAA Security must be assigned to a specific person (i.e.: the HIPAA Security Officer). This individual is responsible for the overall management of ePHI (electronic protected health information) security and the promotion of enterprise-wide security and accountability at Crouse. Crouse Hospital must perform periodic evaluations in order to provide assessments of the safeguards placed within the organization. Crouse Hospital must implement reasonable and appropriate policies and procedures to comply with the HIPAA Security rules and standards. Lastly, Crouse Hospital must document our process for guarding the integrity, confidentiality, and availability of ePHI. This includes activities or actions that are conducted based on our policies and procedures.

Assigned Security

The HIPAA Security Officer (HSO) is responsible for maintaining a comprehensive information security and privacy program related to electronic protected health information (ePHI). The HSO has the authority to ensure the organization complies with statutory and regulatory requirements and standards regarding information storage, access, security and privacy (HIPAA, HITECH, ISO, etc.). The HSO will develop and enforce HIPAA HITECH standards, documentation requirements, Corporate Compliance, policies and procedures, and will partner with IT in these matters. The HSO will assist and lead other Corporate Compliance related projects as needed. The Crouse Hospital job description on file in Human Resources further defines the duties and responsibilities of the HIPAA Security Officer.

Evaluation

Evaluations will be performed on regular basis determined by the HIPAA Security Officer. Evaluations will be conducted to discover any and all security issues impacting the Hospital. This process will also be evaluated when business practices, rules and regulations change and will be done at least annually. All employees, third party affiliates and business associates will fully cooperate by providing accurate

information as part of the process.

Some examples of elements in the evaluation process include:

- Review of findings and plans during previous evaluations
- Review of P&P which are updated annually, forms and templates
- Review of the disaster recovery plan and emergency mode operations
- Staff/organization training evaluation
- Review of mitigation plans
- Information system activity
- Workforce access (including remote access) and authentication mechanisms
- Physical safeguard review
- Privacy and Security incidents
- Workforce and third party termination access activity

Policies and Procedures

Crouse Hospital will maintain policies and procedures required by the HIPAA Security Rule. In order to continue compliance with these rules, the Hospital will address and evaluate these policies on a regular basis. Both required and addressable policies will be created as necessary. The submitter of any new policy should make every effort to determine if the topic is covered by an existing policy and procedure. The HIPAA Security Officer will be responsible for the creation and review of these policies, along with the Policy and Procedure review team. Policies and procedures will be housed within Crouse Hospital's policies and procedures' document portal.

Documentation

The HSO will be responsible for the documentation of these activities. Official forms created by the HSO will be reviewed and added to the Hospital Documents portal. All other HSO-related documents will be housed within the Risk Management department for record-keeping and referencing purposes.

Procedure

Not Applicable

References

HIPAA Security Rule 45 CFR § 164.308(a)(2) – Assigned Security Responsibility

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

CMS Minimum Security Requirements – Acceptable Risk Safeguards

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.

Addendums, Diagrams & Illustrations

Not Applicable