General Information

Policy Name:	HIPAA: Sanction
Category:	Risk Management
Applies To:	Crouse Hospital Employees, Vendors, Physicians, and Volunteers
Key Words:	Sanctions, HIPAA Security, ePHI, Violation
Associated Forms & Policies:	Electronic Communication Resources: Acceptable Use (P1181) Written Information Security Program (WISP) (P1339)
Original Effective Date:	01/01/12
Review Dates:	01/29/16, 01/11/20, 01/10/22, 01/13/23, 01/12/24
Revision Dates:	05/09/16, 03/06/17, 01/12/18
This Version's Effective Date:	01/12/18

Policy

Organizations that house and/or utilize electronic Protected Health Information (ePHI) are required by the HIPAA Security Rule (45 CFR 164.316) to have sanctions in place if security policies and procedures are not followed. Employees of Crouse Hospital have the responsibility to protect ePHI from unauthorized access, disclosure, or security breaches within the hospital. Failure to do so could result in potential harm to patients and/or Crouse Hospital.

The purpose of this policy is to indicate the proper sanctions if an employee fails to comply with Crouse Hospital ePHI security policies and procedures. If a violation does occur, employees will be subject to the sanctions listed in this document. Hospital employees who access patient data for job purposes have the responsibility to understand what is required of them to protect patient data.

If a violation has been discovered or reported, an investigation will be conducted by members of the Information Technology (IT), Risk Management, and Human Resources (HR) Departments to determine if a violation has occurred and if so, the severity of the violation as well as those involved. All investigations will be documented and stored for record-keeping purposes.

Crouse Hospital reserves the right to implement any and all appropriate sanctions necessary after determining the level and severity of the violation through the investigation process. Crouse Hospital also reserves the right to review each violation and determine whether the employee will be subject to a Police/FBI investigation as well possible fines/jail, dependent upon the investigation.

Procedure

Reporting

Employees at Crouse Hospital have the responsibility to report any known violation of ePHI. Failure to report a known ePHI violation may result in disciplinary action as unreported violations could have severe consequences to both the affected patient(s) and Crouse Hospital. Remember, reporting a violation on a fellow employee can be made anonymously and your anonymity will be protected throughout the investigation. Please review your employee handbook for more information.

Violations

There are three different levels of violations from minor to severe. Since not all violations are equal, different sanctions may be chosen depending on the severity of the violation as well the context of the violation itself.

Level 1 – Accidental or Inadvertent

An employee accidentally or inadvertently accessed ePHI that was not authorized or puts a patient's security at risk in an accidental manner. Examples include, but are not limited to:

- Leaving an unsecured workstation unattended
- Sending email/faxes containing ePHI to the wrong recipient
- Accessing the wrong Electronic Medical Record (EMR) file
- Leaving a portable device (ex. Hospital-owned laptops, smartphones tablets, etc.) alone in an area of the hospital
- Connecting an unauthorized device to the Crouse Hospital Network to copy ePHI for job purposes without having received approval from the IT and Risk Management departments

Level 2 – Intentional

An employee intentionally accesses or discloses ePHI without the appropriate authorization. The employee was aware they were accessing unauthorized patient information. Examples include, but are not limited to:

- Accessing your own patient file
- Intentional, unauthorized access to family, friends, co-workers, public personality's, or other individual's ePHI files
- Intentionally assisting or allowing another individual to gain unauthorized access to ePHI. This includes, but is not limited to:
    - Giving another individual your unique username/password to access patient data
    - Logging into an EMR system under your unique username/password and allowing another individual to access ePHI

Level 3 – Deliberate with Intent to Harm

An employee deliberately accesses or discloses ePHI without the required authorization with intent to cause physical, emotional, or financial harm to another person or the company. Examples include, but are not limited to:

- Accessing ePHI for a lawsuit, marital dispute, custody dispute, etc.
- Accessing ePHI for intimidation or other discriminatory uses that could bring personal/financial harm to a patient/co-worker
- Any attempt to maliciously gain access to Crouse Hospital Network resources for personal/financial gain, harm to a patient/co-worker, or financial/reputational damage to Crouse Hospital
- Taking patient information for your own business or to give to a competitor

Sanctions

Level 1 Violation

If it is determined that an employee is responsible for a Level 1 violation, the employee will be subject to the following:

- **Counseling for file.**
- **A Verbal and Written Warning** may be performed at the discretion of their Supervisors, HR, IT, and the Risk Management Department.

Once a written warning and/or counseling/education are complete, it will be documented and placed in the employee's file in the HR department for record-keeping purposes. The Risk Management Department will also keep a copy of the written warning and/or counseling/education for reference.

Level 2 Violation

If it is determined that an employee is responsible for a Level 2 violation, the employee will be subject to the following:

- **A Verbal and Written Warning.**
- **Possible Suspension** may be performed at the discretion of their Supervisors, HR, IT, and the Risk Management department.

Level 3 Violation

If it is determined that an employee is responsible for a Level 3 violation, the employee will be subject to the following:

- **Suspension.**
- **Possible Termination** may be performed at the discretion of their Supervisors, HR, IT, and the Risk Management department.

Depending on the severity of the violation, an employee may also be subject to the following:

- **Possible Investigation by the Police and/or FBI.**
- **Possible Fines and/or Jail for the employee**.

References

45 CFR 164.316 – Policies and procedures and documentation requirements

CMS Minimum Security Requirements – Acceptable Risk Safeguards

Definitions

Sanction: A penalty for breaking or not following a rule or law.

Addendums, Diagrams & Illustrations

Not Applicable