General Information

Policy Name:	HIPAA: System Access Audits
Category:	Risk Management – Corporate Compliance
Applies To:	Individuals that Access Electronic Protected Health Information (ePHI)
Key Words:	Audit, HIPAA, Security, Controls, FairWarning
Associated Forms & Policies:	HIPAA Audit Inappropriate Access Counseling (Doc #5831)
Original Effective Date:	04/01/03
Review Dates:	01/26/16, 12/30/24
Revision Dates:	09/01/05, 07/01/06, 09/01/06, 09/01/07, 01/01/10, 07/01/11, 05/01/12, 06/02/17, 06/02/19, 06/02/21, 10/31/22, 01/26/23, 01/23/24
This Version's Effective Date:	01/23/24

Policy

Crouse Hospital will audit and review inappropriate system access for various systems that are used to house ePHI and patient financials information.

Crouse Hospital reserves the right to audit any patient files to determine whether or not a HIPAA violation has occurred.

FairWarning

The HIPAA Security Officer (HSO) will perform audits for the Soarian Clinicals electronic medical records (EMR) system through the FairWarning auditing system. Reports are generated on a weekly/monthly basis as well as ad-hoc audits that are performed wherever necessary. The auditing reports include, but not limited to:

- Same Name Reports
- Same Address Reports
- Co-Worker Snooping Reports
- Manager/Supervisor-Employee Reports
- Excessive Patient Access Reports
- VIP Reports
- Ad-Hoc reports wherever needed

The HSO will create, change, and/or remove reports as necessary to improve the oversight and auditing process for Soarian Clinicals.

OneContent

The document imaging system OneContent will also be audited on a monthly basis. OneContent Application Administrators will generate a monthly audit report and send it to the HIPAA Security Officer for review. The patients on the report will be Crouse Hospital employees. The HIPAA Security Officer will also perform ad-hoc audits wherever necessary utilizing the OneContent auditing tools.

Regional Health Information Organization (RHIO)

The audit for inappropriate access to the Regional Health Information Organization (RHIO) will be performed and supplied by HeatheConnections. HeatheConnections will provide audit reports. A Corporate Compliance employee will review the reports. The Compliance employee will review these to verify accuracy, privacy violations, etc. In addition, Crouse may request and receive from HealtheConnections an audit log for any provider/user or patient if there is any indication that the information has been accessed inappropriately.

Procedure

1. The HIPAA Security Officer will review the audit reports for FairWarning and OneContent. Any potential violation will be documented by the HIPAA Security Officer which will then be reviewed with the Director of Corporate Compliance/Privacy Officer. Managers and/or Directors will be asked by the Privacy Officer to investigate the potential violations to determine whether or not access was work appropriate.

2. If the access was work appropriate, the Privacy Officer will document the finding as appropriate and no further action will be required.

3. If access for any of these systems are found to be a breach of confidentiality, (i.e. the employee did not need to access that information in order to perform their job duties) the Director or designee of that department will be notified by the Privacy Officer and the following will occur:

    a. The employee breaching confidentiality will be given counseling. The Manager/Director will use counseling Doc #5831 and it will include; wording that the employee understands that access includes self, family members, co-workers, neighbors, etc. It will include wording that directs the employee to protect their computer passwords, and to log off the computer appropriately.

    b. A copy of the Audit and Compliance policy should also be given to the employee at the time of counseling. A copy of the counseling Doc #5831 must be forwarded to the Human Resource and Corporate Compliance departments to maintain on file.

    c. The employee will then reach out to the Privacy Officer either by phone or email for additional discussion.

4. If a second violation occurs after the counseling, the next disciplinary step will be; suspension if the employee is accessing their own information, termination if the access is another individual other than themselves. If a third violation occurs where the employee is accessing their own information, the disciplinary step is termination.

5. All documentation of the results of these audits will be maintained as well as notes on investigations that were done for improper access as record of the audit. A database will be kept in Corporate Compliance and reviewed by the HIPAA Privacy and HIPAA Security Officer.

6. Investigations into allegations of inappropriate disclosure can and will be made at any time. Human Resources, along with Corporate Compliance will interview and investigate all complaints. If the allegations are true, Human Resources will follow the same guidelines as posted above. Any counseling that will occur is documented using Doc #5831. Any failure to improve will lead to further disciplinary action up to and including discharge/termination.

References

HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls

HIPAA Security Rule 45 CFR § 164.308(a)(1)(ii)(D) – Information System Activity Review

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

CMS Minimum Security Requirements – Acceptable Risk Safeguards

Definitions

Audit: An inspection of a patient file to determine whether or not an individual accessed the final inappropriately and/or in an unauthorized manner.

Addendums, Diagrams & Illustrations

Not Applicable