General Information

Policy Name:	HIPAA - Business Associates Uses & Disclosures
Category:	Risk Management – Corporate Compliance
Applies To:	All individuals who work with third-party vendors/organizations that may access, store, create, alter, or remove Crouse Hospital patient data.
Key Words:	BAA, patient data, third-party vendors, PHI, contract
Associated Forms & Policies:	HIPAA BAA (Doc #7564)
Original Effective Date:	02/01/03
Review Dates:	12/01/07, 01/25/16, 02/18/20, 02/08/23, 04/11/25
Revision Dates:	02/01/12, 02/19/18, 02/08/22, 02/05/24
This Version's Effective Date:	02/05/24

Policy

General

It is the policy of Crouse Hospital to ensure that any potential Business Associate that may access, transmit, and store electronic Protected Health Information (ePHI) of Crouse Hospital follow HIPAA Security safeguards and requirements when using and disclosing ePHI.

Crouse Hospital will enter into a Business Associate Agreement (BAA) if the Business Associate accesses Hospital ePHI in any manner as per their functions and/or services. The BAA between the Business Associate and Crouse Hospital must indicate that the Business Associate will use the necessary administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Crouse Hospital ePHI as required by the HIPAA Security Rule (45 CFR 164.302 through 164.318) and HIPAA Privacy Rule (45 CFR 162.502, 162.504).

A BAA must be signed the by the Business Associate before they are allowed to access Crouse Hospital patient data. Failure to do so could leave Crouse Hospital liable for any potential disclosure or breach of ePHI before the BAA has been completed.

All BAAs will be saved for record-keeping purposes at a minimum of six years and will be accessible for review or reference through the Crouse Hospital Contract Portal.

Crouse Hospital reserves the right to terminate any BAA if the Hospital determines that the Business Associate has violated a term within the contract and/or HIPAA and the Business Associate has not taken steps to cure the violation. Refer to the HIPAA BAA (Doc #7564) for more information.

Business Associate Agreement Requirements

Prior to allowing any Business Associate access to Hospital ePHI, Crouse Hospital must obtain assurance from the Business Associate that it will protect Hospital ePHI in the form of a written agreement. The agreement will include the following provisions:

- Business Associates will comply with all provisions of HIPAA Security Rule (45 CFR 164.302

through 164.318) and all provisions of the HIPAA Privacy Rule (45 CFR 162.502, 162.504).

- Protected Health Information will not be used or further disclosed other than as permitted or required by the contract or law.
- The business associate will use appropriate safeguards to prevent use or disclosure of the information other than as provided in the contract.
- The business associate will report to Crouse Hospital any use or disclosure of protected health information other than as provided in the contract.
- Any agent or subcontractor that works on behalf of the business associate will be responsible for following the same guidelines that were set for the business associate.
- The business associate will be aware of the amendment policies for protected health information at Crouse Hospital and will comply in the same manner.
- The business associate will be aware of the accounting of disclosure policies for protected health information at Crouse Hospital and will comply in the same manner.
- The business associate will be aware of the necessary information needed to present to the Secretary of Health and Human Services (HHS) in a case where Crouse Hospital must provide evidence of compliance.
- The business associate will properly destroy all protected health information at the time of termination of contract between itself and Crouse Hospital.

Failure to follow any of these provisions could result in the potential unlawful disclosure or breach of Crouse Hospital ePHI.

Business Associate Agreement Exceptions

In certain situations, The HIPAA Privacy Rule stipulates that Crouse Hospital is not required to have a Business Associate sign a BAA. These can include:

- Disclosures by a covered entity to a health care provider for treatment of the individual.
- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.
- The collection and sharing of protected health information by a health plan that is a public benefits program (ex. Medicare) and an agency other than the agency administering the health plan (ex. Social Security Administration) that collects ePHI to determine eligibility /enrollment (or determines eligibility/enrollment) for the government program, where the joint activities are authorized by law.
- An organization is a conduit for protected health information and does not review any of the data, for example, the US Postal Service.
- An organization whose functions/services do not involve the use or disclosure of ePHI (ex. Janitorial services or electrician)

There may be other instances where a BAA may not be needed. It is the responsibility of Crouse Hospital to review all Business Associates to determine whether or not a BAA is needed prior to utilizing any functions or services.

Procedure

1. Crouse Hospital will evaluate the business associate to determine whether or not a BAA is necessary. If

the vendor is utilizing Crouse Hospital patient data in any manner, then the Business Associate and Crouse Hospital will need to sign a BAA.

2. Prior to the signing and implementation of the BAA, if the employee/department working with the Business Associate has not already done so, they will need to contact the HIPAA Security Officer to perform a risk assessment to determine whether or not the Business Associate has enough security measures in place to protect the confidentiality, integrity, and availability of Crouse Hospital patient data.
3. Once it has been determined by the HIPAA Security Officer's risk assessment that the Business Associate's potential risks are acceptable, the respective department(s) working with the Business Associate will send them a copy of the HIPAA BAA (Doc #7564) for review and signature.
4. If the Business Associate wishes to use their own BAA, the Director of Risk Management, Policy/Procedure & Contracts Administrator and/or HIPAA Security Officer must review the Business Associate's BAA to determine whether or not there are sufficient and appropriate safeguards to protect Crouse Hospital ePHI. If the BAA does not adequately safeguard Hospital ePHI, Crouse Hospital may request changes within the Business Associate's BAA or may request the Business Associate use our BAA instead.
5. Once the BAA has been signed by both parties, the Business Associate will be allowed to access, store, and/or transmit Crouse Hospital patient data for the agreed-upon purposes indicated through business contracts.
6. The BAA will be submitted to the Crouse Hospital Contract Portal for record-keeping and reference purposes for a minimum of six years.

References

HIPAA Security Rule 45 CFR § 164.308(b)(1) - Business Associate Contracts and Other Arrangements - Written Contract or Other Arrangement

HIPAA Security Rule 45 CFR § 164.314(a)(1) - Business associate Contracts or Other Arrangements - Business Associate Contracts

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

CMS Minimum Security Requirements – Acceptable Risk Safeguards

Hospital Cybersecurity Requirements 10 NYCRR 405.46 Hospital Cybersecurity Requirements
Section 405.46 - Hospital Cybersecurity Requirements | New York Codes, Rules and Regulations

Definitions

Business Associate: A person (non-employee) or entity that provides services, or performs functions, to a covered entity that involves access by the person/entity to protected health information.

Business Associate Agreement (BAA): A contracted agreement between a covered entity and a non-covered person or entity that indicates what is required of the non-covered person or entity to secure and protect the covered entity's patient data for their functions and/or services.

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