Stony Brook Medicine Administrative Policy and Procedures

Subject: LD0057 Business Associate Agreements	**Published Date:** 04/26/2022
Leadership	**Next Review Date:** 04/26/2025
Scope: SBM Stony Brook Campus	**Original Creation Date:** 03/11/2003

Responsible Department/Division/Committee:

SBUH HIPAA Privacy Office

Policy:

Stony Brook University Hospital (SBUH) employs processes to ensure that vendors/contractors/agents acting as a Business Associate, enter into a Business Associate Agreement (BAA) with SBUH. The SBUH BAA provides satisfactory assurances to SBUH that the vendor/contractor/agent appropriately safeguards the protected health information/electronic protected health information (PHI/ePHI) the BAA creates, receives, transmits and/or stores on behalf of SBUH in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

Definitions:

Business Associate (BA) - a person or entity who is not a member of SBUH's workforce who on behalf of SBUH, creates, receives, transmits and/or stores PHI/ePHI in the performance of or assisting in the performance of a function or activity involving the use or disclosure of PHI/ePHI.

SBUH Business Owner – The department Manager/Administrator responsible for contracts/purchases for their department.

Protected Health Information (PHI) - Any information, including but not limited to, specimens, radiographs, photographs, any portion of the paper or electronic medical record or research data that contains patient identifiers; such as name, medical record number, social security number, date of birth, encounter number, test results, diagnoses, dates when services were provided, dates of admission, dates of discharge, date of death, etc., that relates to the past, present or future physical or mental health condition of an individual, the

provision of health care to an individual, or payment for the provision of health care to an individual. This definition applies to information that is spoken, written or electronic in form and either directly identifies the individual or could reasonably be used to identify the individual. Any form of information that can identify an individual who has received, is receiving or will be receiving health care.

Workforce member - An employee, volunteer, trainee, or other individual affiliated with SBUH whose work is under the direct control of SBUH regardless of whether they are paid by SBUH.

Procedures:

A. Each SBUH Business Owner contracting with and/or paying a vendor, company or agent defined as a BA as noted above; is responsible to inform Hospital Purchasing that a Business Associate Agreement is required.

1. RFPs/IFBs must contain language addressing the requirement to enter into a BAA w/ SBUH

2. Any Purchase Order (PO) paid to a vendor, company or agent functioning as a BA must have a BAA in place.

3. All contracts with a vendor, company or agent functioning as a BA must have a BAA in place.

B. Business Associate Agreement Content:

1. Is written in compliance with the HIPAA regulation requirements.

2. Is updated from time-to-time by the Chief HIPAA Privacy Officer, SBU Legal Counsel and/or SUNY Counsel. Each time the Agreement is updated the document is dated and the updated agreement is sent to Hospital Purchasing to replace the former version.

3. Hospital Purchasing sends a copy of the fully executed BAA and the completed contract highlight sheet or standalone annual POs, as appropriate, to the HIPAA Privacy Office for documentation into HIPAA Privacy Officer tracking solution.

4. The HIPAA Privacy Office notifies the SBUH Business Owner And Hospital Purchasing of a pending contract termination. This prompts action by the Business Owner to ensure SBUH PHI is either returned, destroyed (completed certificate of destruction received from vendor), an agreement to maintain protections is provided by the vendor or renewed contract with the same vendor is in place.

C. Business Associate Agreement/Contract Termination:

1. The SBUH Business Owner at the termination of the contract, is responsible to ensure the return or destruction of all PHI in the vendors possession. A vendor destroying the PHI in their possession must complete and submit to the SBUH Business Owner the Certificate of Destruction provided to the SBUH Business Owner at the time of contracting.

2. Hospital Purchasing may authorize SBUH's termination of the contract if SBUH determines that the BA has violated a material term of the contract and if such termination is appropriate and consistent with the statutory obligations of SBUH or its BA.

D. Treatment Relationships – A BAA is not needed for disclosures by SBUH to a healthcare provider concerning the treatment of a patient.

E. Compliance – In order to ensure compliance, SBUH will:

1. Investigate complaints or other information containing substantial and creditable evidence of violation(s) by a BA.

2. Take reasonable steps to cure a breach or violation of which it becomes aware. If such steps are unsuccessful, SBUH will:
   a. Terminate the contract; or
   b. Report the problem to the Secretary of HHS, if termination is not feasible.

F. SBUH as the BA – If SBUH is a BA of another covered entity; SBUH is obligated to comply with BA requirements as stated in the terms of the contract.

G. Documentation – All BA contracts are documented and retained in accordance with State University of New York (SUNY) record retention

guidelines.

H. Periodically, the Stony Brook Medicine Chief HIPAA Privacy Officer, or designee(s), surveys the Stony Brook Organized Health Care Arrangement to ensure agreements are in place with vendors, contractors, agents and organizations with whom PHI is shared.

Forms: (Ctrl-Click form name to view)

2019 SUNY Business Associate Agreement
Contract Highlight Sheet
Certificate of Destruction
(Available through Hospital Purchasing 444-4050)

Policy Cross Reference: (Ctrl-Click policy name to view)

None

Relevant Standards/Codes/Rules/Regulations/Statutes:

Health Insurance Portability and Accountability Act 1996 (HIPAA), 45 CFR §164.502 (e) (1)

References and Resources:

None