SUNY DOWNSTATE HEALTH SCIENCES UNIVERSITY (DOWNSTATE)

POLICY AND PROCEDURE

No. HIPAA-3

Subject: **BUSINESS ASSOCIATE AGREEMENTS**

Page: 1 of 4

Prepared by: Shoshana Milstein, CHC RHIA CHP CCS

Original Issue Date: 12/2002

Reviewed by: Alexandra Bliss, CHC

Supersedes: 12/2016

Effective Date: 09/2024

Committee Approval:
Executive Performance Improvement Council (EPIC)

TJC Standards:
TJC Standards: RI.OI.OI .01: The hospital respects, protects, and promotes patient rights.
LD.04.02.03: Ethical principles guide the hospital's business practice.

Issued by: Regulatory Affairs

I. PURPOSE

To ensure that all business associates (BA) enter into an appropriate contract with SUNY Downstate Health Sciences University (Downstate) that will provide satisfactory assurance to Downstate that the business associate will appropriately safeguard the protected health information (PHI), in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.

II. POLICY

A. Business Associate Agreement (BAA) Content- The contract between Downstate and a BA must:

1. Establish the permitted and required uses and disclosures of the information. The contract may not authorize further use or disclosure in a manner that would violate the HIPAA standards, except that:
   a. The contract may permit the BA to use or disclose PHI for the proper management and administration of the BA; and
   b. The contract may permit the BA to provide data aggregation services relating to Downstate's health care operations.

2. Provide that the BA will:
   a. Accept direct liability for compliance with the HIPAA Rules related to impermissible uses and disclosures, failure to provide breach notification to the covered entity, failure to provide access to a copy of electronic PHI to either the covered entity or the individual/ designee, failure to disclose PHI where required by the Secretary to investigate or determine compliance with the HIPAA Rules, failure to provide an accounting of disclosures and failure to comply with the requirements of the Security Rule;
   b. Not use or further disclose the information other than as stated in the contract or as required by law;
   c. Use appropriate safeguards, including administrative, physical and technical safeguards, to prevent unauthorized use and disclosure other than as provided in the contract and to protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of the covered entity;
   d. Report to Downstate any use or disclosure of information not provided for by the contract or any security incident of which it becomes aware, including breaches of unsecured PHI as required by the breach notification rules;
   e. Ensure that any agents and subcontractors to whom it provided PHI received from, or created by the BA on behalf of, Downstate agrees to the same restrictions and conditions provided in the contract by executing a BAA with the subcontractor and requiring those subcontractors to execute a BAA, detailing the same permitted uses/ disclosures, with any further downstream subcontractor(s);
   f. Make available and provide access of PHI to a patient, when requested;
   g. Make available PHI for amendment and incorporate any amendments to PHI, as necessary;
   h. Make available the information required to provide an accounting of disclosures;
   i. Make its internal practices, books and records relating to the use and disclosure of PHI received from, or created on behalf of, Downstate available to the Secretary of the Department of Health and Human Services (HHS) for purposes of determining Downstate's compliance with the HIPAA Privacy standards; and
   j. If feasible, at termination of the contract, return or destroy all PHI received from, or created on behalf of, Downstate that the BA still maintains in any form. The BA must not retain any copies of the information.
   k. If not feasible, the BA must extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

3. Authorize Downstate's termination of the contract if Downstate determines that the BA has violated a material term of the contract.
   a. If termination is not feasible, Downstate is required to notify the Secretary of the Department of Health and Human Services (HHS) of the un-cured breach.

B. Permitted Uses & Disclosures

1. The contract may permit the BA to **use** the information, if necessary:
   a. For the proper management and administration of the BA; or
   b. To carry out the legal responsibilities of the BA.

2. The contract may permit the BA to **disclose** the information for the above purposes, if:
   a. The disclosure is required by law; or
   b. The BA obtains reasonable assurances from the recipient that:
      i. The information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient;
      ii. S/he will notify the BA of any breaches of confidentiality of which s/he becomes aware.

C. Treatment Relationships- A BA agreement is not needed for disclosures by Downstate to a healthcare provider concerning the treatment of a patient.

D. Compliance- In order to ensure compliance, Downstate will:

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

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

E. Downstate as the BA- If Downstate is a BA of another covered entity, it must comply with all the terms stated in the contract.

F. Documentation- All BA contracts must be documented and retained, as appropriate.

III. DEFINITION(s)

Business Associate- A person or entity who is not a member of Downstate's workforce who:

1. On behalf of Downstate, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management and repricing; health information exchanges and health storage facilities;
2. Is a contractor or subcontractor that creates, receives, maintains or transmits PHI on behalf of Downstate or one of its business associates; or
3. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to Downstate, where the provision of the service involved the disclosure of PHI from Downstate.

II. RESPONSIBILITIES

It is the responsibility of all medical staff members and hospital staff members to comply with this policy. Medical staff members include physicians as well as allied health professionals. Hospital staff members include all employees, medical or other students, trainees, residents, interns, volunteers, consultants, contractors and subcontractors at the hospital.

III. PROCEDURE/GUIDELINES

All new contracts and renewal of contracts for services that may involve PHI will incorporate the Downstate BAA template as an exhibit to and as a part of such contract. Both the BAA and an authorized signatory at Downstate must sign all BAA's. The Office of Contracts and Procurement is responsible for coordinating the execution of and maintaining all completed BAA forms.

In addition, the Office of Contracts and Procurement will, on an annual basis, review a current Vendor Disbursement Report to identify any additional vendors that may require a BAA.

If a vendor proposes revisions to the language in Downstate's standard BAA, DMC's HIPAA Privacy Officer and/or Counsel will review such proposed revisions for acceptability.

IV. ATTACHMENTS

Business Associate Agreements: Downstate as Business Associate, Downstate as Covered
Entity

V. REFERENCES

Standards for Privacy of Individually Identifiable Health Information, 45 CFR §164.502(e), §164.504(e)

DATE REVIEWED	REVISION REQUIRED (CLICK BOX)		RESPONSIBLE STAFF NAME AND TITLE
	YES	NO	
9/2013	☒	☒	Shoshana Milstein, AVP, Compliance & Audit
92016	☐	☒	Shoshana Milstein, AVP, Compliance & Audit
12/2016	☐	☒	Shoshana Milstein, AVP, Compliance & Audit
9/2024	☐	☒	Alexandra Bliss, CHC, Compliance & Audit