POLICY TITLE: HIPAA Business Associate Policy	SYSTEM POLICY AND PROCEDURE MANUAL
POLICY #: 800.19	**CATEGORY:** Compliance and Ethics
System Approval Date: 4/25/2024 **Site Implementation Date:** 6/03/2024	**Effective Date:** 09/15/2016 **Last Reviewed/Approved:** 05/2022
Prepared by: Office of Legal Affairs, Procurement Office of Corporate Compliance	**Notations:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this document is to have the Health Insurance Portability and Accountability Act ("HIPAA") regulations permit health care providers such as Northwell Health and its affiliates to share health information with their contractors for purposes of "treatment, payment and health care operations." The HIPAA regulations seek to ensure that these third parties referred to as Business Associates ("BAs") adhere to the basic protections imposed by the regulations and that there are appropriate privacy and security safeguards when protected health information ("PHI") is shared with business partners.

The purpose of this policy to identify the process by which PHI can be appropriately released to BAs, and the mechanism for developing and maintaining contractual agreements with BAs regarding their responsibilities under the HIPAA regulations.

POLICY STATEMENT

It is the policy of Northwell Health that as a Covered Entity, Northwell Health must disclose PHI to a BA and must allow such individual or organization to create, transmit, maintain, process, or receive such information on its behalf if Northwell Health obtains satisfactory assurances that the BA will appropriately safeguard the information.

It is the policy of Northwell Health that all BAs must enter into a Health System approved Business Associate Agreement ("BAA") or addendum unless it is determined a BAA is not required.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Donald and Barbara Zucker School of Medicine at

Hofstra/Northwell or the Hofstra Northwell School of Nursing and Physician Assistant Studies conducting research on behalf of the Zucker School of Medicine on or at any Northwell Health facility.

DEFINITIONS

Business Associate ("BA"): A person or entity that performs certain functions or activities, or provides services that creates, receives, maintains, processes or transmits PHI on behalf of, or to Northwell Health and is an external person or entity.

Examples of BA functions or activities can include, but are not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and software hosting of PHI. Examples of BA services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

If you have any questions regarding whether a person or entity's function qualifies as a BA, contact the Office of Procurement.

Business Associate Agreement ("BAA"): A legally binding agreement entered into by a Covered Entity and BA that establishes permitted and required uses and disclosures of PHI, provides obligations for the BA to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Covered Entity: A facility that conducts Health Care Operations involving the creation and transmission of PHI. Each facility in Northwell Health which conducts Health Care Operations is its own Covered Entity. These Covered Entities are collectively considered an Organized Health Care Arrangement which allows each of the included Covered Entities to share PHI for treatment, payment and health care operations without the requirement of a BAA between Covered Entities.

Protected Health Information ("PHI"): Any oral, written, or electronic individually identifiable health information. PHI is information created or received by Northwell that (i) may relate to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and (ii) identifies the individual who is the subject or based on which there is a reasonable basis to believe that the individual who is the subject can be identified. The *Health Insurance Portability and Accountability Act* (HIPAA) further clarifies that PHI includes information that identifies the individual by one or more (depending on context) of the following 18 identifiers:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes except for the initial three digits of a ZIP code in certain situations;
3. All elements of a date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;

7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers;
13. Medical device identifiers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Subcontractor: A person or entity to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

PROCEDURE

Obtaining and Securing Business Associate Agreements

1. A BAA is required for all BAs unless otherwise outlined herein.

2. Only the Office of Procurement, Enterprise Digital Services ("EDS") and the Office of Legal Affairs have the authority to secure BAAs.

3. In accordance with Northwell Health Administrative Policy #103.01 Approval and Signatory Authority, only authorized officials of Northwell Health can sign BAAs. If an authorized official has a designee(s), such designee(s) may sign the BAA on the authorized official's behalf.

4. The Office of Procurement maintains Northwell Health's official repository for BAAs.

5. When it is determined that a BAA is required, pursuant to an underlying agreement and or request for services, the department where the services are being rendered will be responsible to provide the following information to the Office of Procurement, EDS or the Office of Legal Affairs, as applicable, depending upon the nature of the service:
    - The name and contact information of the BA and Health System business owner/end user/requestor of services;
    - Description of services being provided by the BA; and
    - Type of PHI to be created, maintained, received or processed by the BA, and how the PHI is being handled or stored by the BA.

6. If applicable, EDS will evaluate BA's technical security controls and safeguards prior to entering into a BAA. Furthermore, BAs will be subject to information security reviews as indicated by EDS Standard Operating Procedures, and if applicable, will be required to bind all Subcontractors that use or disclose Health System PHI to the same restrictions and conditions

regarding PHI as are applicable to BA. *Refer to Policy 900.28, Information Security Reviews of Procured Systems.*

7. Prior to allowing a BA access to Northwell Health's PHI, Northwell Health must execute an underlying agreement for services and a BAA (or addendum) with the BA. The BAA form can be obtained from the Office of Procurement and shall only be used by authorized departments as outlined herein. As per Section 2 above, only the Office of Procurement, EDS, and the Office of Legal Affairs has the authority to issue and secure a BAA on behalf of Northwell.

8. No BAA submitted from an outside organization is authorized for signature unless and until expressly reviewed and approved by the Office of Legal Affairs.

9. If a BAA is required, the BAA must be signed by both parties before the BA performs any services that involve the use and/or disclosure of PHI.

10. In the event a BA refuses to execute a BAA and the BA is not exempt as approved herein, the service agreement cannot be executed and the services may not be performed.

11. Members of Northwell Health as defined herein that become aware of a breach or a material violation of a BAA by the BA, must report such finding to the Office of Corporate Compliance, whose contact information is set forth below, immediately in efforts to ensure immediate action and reasonable steps to cure the breach or end the material violation.

12. Members of Northwell Health will follow Policy #800.17 (HIPAA and State Privacy Breach Notifications) for any breach by a BA.

13. If a person or an entity provides services requiring the use or disclosure of PHI and meets the definition of a BA, and a member of Northwell Health becomes aware that no agreement or BAA has been secured, the individual must notify the Office of Corporate Compliance immediately. The Office of Procurement, EDS and the Office of Legal Affairs will then negotiate any legally-required agreements, if applicable, and date such agreements as of the date in which PHI was first received by the BA.

14. In addition to the BAA requirement, if a Business Associate must access Northwell Health's electronic systems, applications and/or infrastructure, pursuant to an underlying agreement in order to provide services, the BA may be required to sign the appropriate confidentiality agreement(s). This may include a Confidentiality Agreement, Non-Disclosure Agreement, a BA Agreement or other documents as deemed necessary. *Refer to Policy 900.00, Acceptable Computer Use Policy.*

Identifying when a Business Associate Agreement Is Not Required

A BAA is not required if the individual or entity meets one of the following scenarios listed below or you obtain written approval from the Office of Legal Affairs:

a) member of Northwell Health's workforce;
b) a health care provider (whether unaffiliated or affiliated with Northwell Health) who discloses PHI for treatment purposes;

c) functions or provides services without involving the use or disclosure of PHI and where access to PHI would be incidental if at all (e.g., cleaning services);
d) acts merely as a conduit for PHI such as the United States Postal Service or a private courier;
e) discloses PHI for research purposes either with patient authorization or pursuant to a valid research waiver;
f) a financial institution that processes consumer-conducted financial transactions by debit, credit, check or other electronic funds transfer;
g) an insurer where Northwell Health discloses PHI to a health plan for payment purposes or accepts a discounted rate to participate in the health plan's network; or
h) is exempt as per HIPAA.

ENFORCEMENT

In compliance with the HIPAA Privacy Rule, violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and in the Bylaws, Rules and Regulations of the Medical Staff.

CONTACT INFORMATION

Office of Corporate Compliance	516-465-8097
Compliance Help Line	800-894-3226
	www.northwell.ethicspoint.com

Training
The Office of Corporate Compliance will provide training on HIPAA on, at least, an annual basis.

Document Retention
Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of its creation.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)
- Final HIPAA Omnibus Rule (78 Fed. Reg. 5566)
- Northwell Health-Human Resources Policy, Part 5, Discipline and Standards of Conduct
- Northwell Health-Human Resources Policy, Part 5-3 Workforce Conduct/Progressive Discipline
- Bylaws, Rules and Regulations of the Medical Staff
- Northwell Health System Policy #800.17 – HIPAA and State Privacy Breach Notifications
- Northwell Health System Policy # 100.97 - Records Retention and Destruction Policy
- Northwell Health Policy #900.00 – Acceptable Computer Use Policy
- Northwell Health Policy #900.28 - Information Security Reviews of Procured Systems

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES
N/A

ATTACHMENTS
N/A

FORMS
N/A

APPROVAL:	
Northwell Health Policy Committee	3/26/2024
System PICG/Clinical Operations Committee	4/25/2024

Standardized Versioning History:
Approvals: * =Northwell Health Policy Committee; ** = PICG/Clinical Operations Committee; ✠ = Provisional; ❖ = Expedited

*07/13	** 8/13
*12/18/15	**01/21/16
*08/25/16	**09/15/16
❖06/18/18	
*05/21/20	**06/18/20
*04/28/22	**05/19/22