Effective Date: **August 1, 2013** Revised: **November 26, 2024**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY, RESEARCH AND SCHOLARLY ACTIVITIES

HIPAA Policies for Healthcare Providers at Covered Components: Policy 3 – Using PHI in Treatment, for Payment and for Health Care Operations; Business Associates

RESPONSIBLE OFFICE

Research Compliance

This Policy 3 is part of the HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components.

3.1 Overview

The policies that follow describe routine and non-routine disclosures. Routine disclosures are those that are made regularly and frequently. For example, using PHI for treatment and to obtain payment for that treatment is a routine disclosure. PHI is also routinely used to manage the health care clinic. Detailed information on HIPAA's rules for these routine uses is provided

in these policies to facilitate the routine activities of the Covered Components.

Non-routine disclosures are rarely encountered. Information on HIPAA rules for non-routine disclosures is provided in polices 4 and 5, below. Covered Components are always encouraged (and in some circumstances required) to contact the BU HIPAA Privacy Officer for guidance and/or approval in these non-routine circumstances.

The disclosure policies also note when disclosures (both routine and non-routine) may or must be made without a written and signed Authorization.

3.2 Minimum Necessary Rule

In most circumstances, when using or disclosing PHI or when requesting PHI from another HIPAA Covered Entity/Component, the BU Covered Component must limit the use or disclosure to that which is necessary to accomplish the intended purpose of the use, disclosure, or request for information.

Exceptions to the Minimum Necessary Rule:

- Disclosures or requests by a health care provider of information *for treatment purposes*. Health care providers use their professional judgment in determining what PHI is needed for treatment purposes;
- Uses or disclosures pursuant to Authorization, because the disclosure should follow the patient's direction in the Authorization;
- Disclosures made to the Secretary of Health and Human Services, which will be made by the BU HIPAA Privacy and/or Security Officers; and
- Uses or disclosures required by law, for example,
    - Mandatory reports of abuse, neglect or domestic violence,
    - Uses and disclosures for governmental health oversight activities,
    - Disclosures for judicial and administrative proceeding and pursuant to subpoena or court order.

In all other circumstances, follow the Minimum Necessary Rule.

3.3 Special Rules for PHI in Limited Data

Sets

A Covered Component may use or disclose a Limited Data Set (defined below) only for the purposes of research, public health, or health care operations, and only after entering into a Limited Data Use Agreement with the recipient.

Definition of Limited Data Set

A limited data set is PHI that excludes the following direct identifiers of the individual or of the individual's relatives, employers, or household members:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

An alternate way of understanding a Limited Data Set is that it is PHI that has been de-identified except for dates, which may be included in a Limited Data Set. Thus, if you try to de-identify data but find you need to retain dates, treating it as a Limited Data Set may be a good option.

Limited Data Sets are frequently used in research.

Data Use Agreement

Contact the BU HIPAA Privacy Officer for a Limited Data Use Agreement either to be used in disclosing BU Covered Component PHI, or in receiving PHI from another entity.

BU researchers may accept Data Use Agreements from other entities disclosing research data to BU only if approved by the BU HIPAA Privacy Officer.

Breaches of Data Use Agreements

If a Covered Component that has disclosed its PHI pursuant to a Data Breach Agreement learns of the recipient's possible breach of the agreement, the Covered Component must first report the matter to the BU HIPAA Privacy Officer, who will work with the Covered Component to take reasonable steps to investigate and, if necessary, cure the breach, end the violation, or discontinue disclosure of the data. If a breach is confirmed, the BU HIPAA Privacy Officer will make any necessary report to the affected individuals and the Secretary of Health and Human Services.

3.4 Patient Authorization Not Needed for Treatment Purposes

Treatment purposes includes providing, coordinating or managing a patient's health care services.

*Minimum Necessary Rule Not Applicable:*When using PHI for Treatment purposes (including disclosing it to other providers for treatment purposes), it is not necessary to limit the use or disclosure to the "minimum necessary". Health care providers should use their professional judgment in accessing, using and disclosing whatever information they deem necessary for treatment purposes.

Research recruitment: Anyone in a Covered Component may approach the Covered Component's patients about participation in research, as that communication is considered part of treatment. However, the treating provider/Covered Component may not provide patient contact information or any other PHI to a researcher outside the Covered Component without

the patient's Authorization.

Provider Treatment Recommendations, Options: A face-to-face communication made by a Covered Component to an individual recommending additional services of the Covered Component or of another Covered Entity/Component falls within the definition of "Treatment." For example, dentists may recommend use of a waterpik; dieticians may recommend certain foods or supplements. Providers and Covered Components are prohibited from accepting payment from any other entity or person to recommend that entity or person's services or products to patients. See Section 4.2: Prohibited Uses of PHI.

3.5 Using PHI for Payment Purposes

Disclosures for Payment Purposes
An authorization is not required to use PHI for payment purposes. Payment purposes include all activities directed at obtaining reimbursement for health care services, such as:

- verifying an Individual's insurance coverages;
- creating the claim;
- sending the claim to the patient and/or the patient's insurer;
- interactions with the patient's insurer for the purpose of obtaining payment;
- processing payments;
- collections activities; and
- evaluating an Individual's eligibility for financial assistance.

Minimum Necessary Rule Applies:When using and disclosing PHI for payment purposes, only the minimum necessary information should be used and disclosed.

3.6 Using PHI for Health Care Operations Purposes

Disclosures for the Covered Component's Operations
An authorization is not necessary to use PHI for the Covered Component's operations, such

as:

- quality assessment and improvement activities (but not generalized research);
- case management;
- human resources, including reviewing the competence and performance of providers and other Workforce members and resolution of internal grievances;
- training of professional and non-professional students;
- accreditation;
- certification;
- licensing;
- credentialing;
- financial management;
- compliance, risk management, auditing and legal services;
- investigations of possible fraud and abuse;
- business development and planning; and
- all other business and administrative activities required for the Covered Component to operate.

Minimum Necessary Rule Applies:When using and disclosing PHI for operations, only the minimum necessary information should be accessed, used or disclosed.

3.7 Routine Disclosures to an Individual's Family and Friends

Patients are entitled to involve family and friends in their care, if they wish, and Covered Components should honor those wishes by disclosing PHI to those persons, to the extent the patient has involved them. Below is guidance on how to manage these disclosures in several types of circumstances in which this may arise.

Specific Authorization
If the patient signs an Authorization to disclose information to another person, the Covered Component should follow that Authorization. For example, if a patient signs an Authorization allowing a Covered Component to share billing and payment information with her spouse, the

Covered Component should honor that Authorization, but may not go beyond it by providing the spouse non-billing/payment information.

Informal Authorization

If an Individual involves a friend or family member in his/her care, the Covered Component may disclose to that person information directly relevant to the nature of the person's involvement with the patient's care, even in the absence of a written Authorization. Providers may honor an Individual's informal request to share his/her PHI with others if:

- the patient is present and requests the Covered Component do so, or
- if the patient is present and does not object, or
- if the provider reasonably infers from the circumstances, based on the exercise of professional judgment that the patient does not object to such disclosure.

For example, if a patient brings a friend to an appointment, it is permissible to discuss the patient's condition, plan of care, and other matters typically discussed in such an appointment with the friend present. But it would not be permissible to provide that friend billing information, if the patient did not involve the friend in billing issues.

While providers may rely on a patient's informal indication of permission to share information, having the patient indicate his/her desires in writing in an Authorization may help avoid confusion and misunderstanding.

Notification Purposes

The Covered Component may use or disclose PHI for purposes of notifying an individual's family member, Legally Authorized Representative, or another person responsible for the care of the patient, of the patient's location, general condition, or death. It may also use and disclose PHI in these circumstances for identifying or locating an individual's family member, Personal Representative or other person responsible for the care of the individual.

3.8 Sharing PHI with the Patient's Other

Providers and Health Plans

Health care providers and health care plans often share information about the patients who are common to both. This is permissible under HIPAA, subject to the following:

Treatment
Treatment includes disclosing PHI to another health care provider who is treating the patient, or who may treat the patient, when the purpose of the disclosure is to provide, coordinate or manage treatment of the patient.

You do not need the patient's Authorization or permission, bit it is a good practice to require a patient to sign an Authorization when releasing records to another health care provider for Treatment purposes because that will confirm the patient's relationship with the other provider. However, when that is not feasible, and when the Covered Component has a good faith belief that the other provider has, had or may be entering into, a treatment relationship with the patient, it is permissible to make the disclosure to the other provider without a signed patient Authorization.

Minimum Necessary Rule Not Applicable: Because this is considered using PHI for Treatment purposes, it is not necessary to limit the use or disclosure to the "minimum necessary". Health care providers should use their professional judgment in accessing, using and disclosing whatever information each deems necessary for treatment purposes.

Payment
Disclosures to an Individual's other health care providers and insurers for purposes of payment are permissible even without patient authorization. This covers all communications with a patient's health plan and all communications with the patient's other health care providers when the purpose relates to payment for health care services of one or more of them.

Minimum Necessary rule applies.

Disclosures for Operations of Other Providers and Covered Components/Entities

HIPAA allows a Covered Component to disclose PHI to another Covered Entity/Component for the operations of that other Covered Entity/Component, but only when all of three of the following apply:

- Each Covered Entity/Component has or had a relationship with the patient whose PHI will be shared; and
- The PHI pertains to that relationship; and
- The disclosure is for one of the purposes listed below:
    - Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (but not research); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; or
    - Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; reviewing health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation; certification; licensing or credentialing activities; or
    - For the purpose of investigating health care fraud and abuse.

The Minimum Necessary rule applies.

This does not occur very often, and Covered Components are encouraged to contact the BU HIPAA Privacy Officer for guidance.

3.9 Disclosing PHI to Business Associates

BU’s Covered Components may engage, or BU may engage on behalf of the Covered Components, entities outside of BU to perform various services. When the services involve the outside entity accessing, using, creating or disclosing PHI held by any Covered Component, those entities are likely to be Business Associates of the Covered Component. The University, including its Covered Components, may not disclose any PHI to Business Associates until a Business Associate Agreement is fully executed.

Business Associate Agreements

The Business Associate Agreement must contain certain elements, which require the Business Associate to maintain the confidentiality of the PHI that it receives, to use and disclose such information only for the purposes for which it was provided, and to comply with the same HIPAA requirements as the Covered Component.

Responsibilities

The *BU HIPAA Privacy Officer and/or Security Officer* will:

- Approve a standard form Business Associate Agreement and make it available to the Covered Components and Support Units; and
- Approve any changes to a Business Associate Agreement.
- Be available to advise Covered Components and Support Units on whether a service provider is a Business Associate; and
- Periodically audit the Business Associate logs and agreements maintained by Covered Components and Support Units.

The *Covered Components* are responsible for:

- Determining whether any service provider it retains, who is external to BU, is a Business Associate, and if so, for ensuring a Business Associate Agreement approved by the BU HIPAA Privacy Officer is fully executed before any PHI is disclosed;
- Contacting the BU HIPAA Privacy Officer to approve any change the terms of the standard approved Business Associate Agreement; and
- Maintaining on the BU HIPAA SharePoint site a log of all Business Associates and copies of all Business Associate Agreements for that Covered Component.

Support Units that retain the services of a Business Associate are responsible for:

- Determining whether the service provider is a Business Associate and if so, entering into a Business Associate Agreement before disclosing any PHI. The Covered Component HIPAA Contact will act as a check and upon becoming aware of a Business Associate retained by a Support Unit, will verify that a Business Associate Agreement was fully executed.

Who is a Business Associate?

HIPAA defines a Business Associate as a person or entity that:

- is not a member of the Covered Component Workforce,
- provides a service, or performs a function, or assists in the performance of a function or activity on behalf of a Covered Component, and
- in performing its duties for the Covered Component, may access, use, create or disclose PHI.

HIPAA does not define which entities or services fall into the Business Associate category; the determination must be made case by case, using the definition above. Following are examples:

Almost Always A Business Associate	**May Be A Business Associate (when services involve PHI)**	**Never A Business Associate**
Claims processing or administration	Management consultants	Members of the Covered Component's Workforce
Billing	Legal services	Other health care providers of the Covered Component's patients, when acting in that capacity; i.e., a health care provider providing health care services. Note that health care providers may perform business services such as billing or consulting for a BU Covered Component; in which case it would be a BA. See column to the left.

Almost Always A Business Associate	May Be A Business Associate (when services involve PHI)	Never A Business Associate
Practice management	Financial, accounting, actuarial, and similar services	Custodians, janitors, couriers, repairmen etc. where access to PHI is not required to perform their services, even if there may be incidental disclosure to them
Data analysis, processing or administration	Data aggregation services, IT services	Financial institutions processing financial transactions (e.g., credit card processing or check clearing)
Utilization review	IT services, including data migration or software or system maintenance	Public health oversight agencies, such as the Massachusetts Department of Public Health, performing health oversight functions
Quality assurance	Collection agencies	Recipients of De-Identified Information or “Limited Data Set”: No Business Associate Agreement is needed when the health information being disclosed or created has been de-identified in accordance with the de-identification standards under the Privacy Regulations, or the health information qualifies as a Limited Data Set disclosed pursuant to a Limited Data Use Agreement

Almost Always A Business Associate	May Be A Business Associate (when services involve PHI)	Never A Business Associate
Transcription services, Answering services	Accreditation organizations	Health care insurers of the Covered Components' patients, when acting in that capacity; Disclosures to health care insurers is allowed for Payment purposes.

Enforcement of Business Associate Agreements

If the Covered Component becomes aware of any breach of a Business Associate Agreement, it must notify the BU HIPAA Privacy Officer to assess whether it is necessary to take steps to cure the breach or terminate the underlying service contract if feasible.

Standard Form

The approved BU standard form of Business Associate Agreement should be used.

If an outside organization or person sends its own form of Business Associate Agreement to be signed, please inform the BA that the PHI belongs to BU and its patients and BU protects it by using its own form. If the Business Associate insists on using its form or requests modifications of the BU template, contact the BU HIPAA Privacy Officer.

BU as a Business Associate

If any Boston University office or department provides services to an outside HIPAA Covered Entity such that the outside entity requests BU sign a Business Associate Agreement, contact the BU HIPAA Privacy Officer, who will determine whether a Business Associate Agreement is needed and if so, may approve it.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies, Procedures, and Guides

- HIPAA
  - HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components
  - HIPAA Policies for BU Health Plans
  - HIPAA Information for Charles River Campus Researchers
- Data Security
  - Data Protection Standards

BU Websites

- HIPAA at Boston University
  - FAQ's
  - Forms for Health Care Providers
  - HIPAA for BU Researchers
  - HIPAA Data Security Tips
  - Report a Possible HIPAA Breach

Categories: Information Management, Privacy and Security, Protected Health Information - HIPAA for BU Healthcare, Research and Scholarly Activities, Research Compliance and Safety