Effective Date: **April 10, 2017**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

HIPAA Policies for BU Health Plans: Policy 3, Routine Use and Disclosure of PHI

RESPONSIBLE OFFICE

Research Compliance

This Policy 3 is part of the HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans.

3.1 Overview of Routine Uses and Disclosures

The policies that follow describe routine and non-routine disclosures. Routine disclosures are those that are made regularly and frequently. The BU HIPAA Privacy Officer is available for guidance and/or approval in 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 Health Plans 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

- Uses or disclosures pursuant to Authorization, because the disclosure should follow the participant'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 oversight activities, or
    - Disclosures for judicial and administrative proceeding and pursuant to subpoena or court order.

In all other circumstances, follow the Minimum Necessary Rule.

3.3 PHI in Limited Data Sets

The BU Health Plans may use or disclose a Limited Data Set (see 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. This occurs very rarely in the BU Health Plans. If the need for a Limited Data Set arises, the BU Health Plans will follow the guidance in the BU HIPAA Policies for Health Care Providers, with the guidance of the BU HIPAA Privacy Officer.

3.4 Routine Use and Disclosure of PHI to BU as Plan Sponsor Without Authorization

Disclosures of PHI by the BU Health Plans to BU are subject to the Minimum Necessary rule.

BU Health Plans have included a separate statement in the Notice of Privacy Practices informing Individuals that PHI may be disclosed to BU.

Disclosure of Summary Health Information

BU Health Plans (or Claims Administrator with respect to BU Health Plans) may disclose summary Health Information to BU as Plan Sponsor without regard to whether the plan documents have been amended, if BU as Plan Sponsor requests the Summary Health Information for the purpose of:

- Obtaining utilization data from a Health Plan for providing coverage under BU Health Plans, or
- Assessing, modifying, amending or terminating BU Health Plans.

Disclosures to BU as Plan Administrator

The BU Health Plans' plan documents:

- Describe the permitted Uses and Disclosures of PHI by BU.
- Specify that Disclosure is permitted only upon receipt of a written certification by BU that the plan documents have been amended in accordance with the HIPAA requirements.
- Provide adequate physical and technical firewalls which identify the employees, classes of employees or other persons under BU control who will have access to PHI and ePHI.
- Ensure that the separation between BU Health Plans and BU is supported by reasonable and appropriate security measures.
- Require that BU report to the BU Health Plans any security incident of which it becomes aware.
- Provide an effective mechanism for resolving any issues of non-compliance by the BU employees or class of employees who will have access to PHI.

BU's Certification that the Plan Documents have been so amended is found at Appendix C.

Disclosure of Enrollment Information

BU Health Plans (or Claims Administrator) may disclose to BU as Plan Sponsor information on whether an Individual is participating in any or all of the BU Health Plans, or is enrolled in or has disenrolled from a the BU Health Plans, without regard to whether the plan documents

have been amended.

All other disclosures of PHI to BU as Plan Sponsor must be authorized by Individuals in writing.

3.5 Routine Use and Disclosure of PHI without Patient Authorization for Treatment Purposes

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

3.6 Routine Use of PHI without Patient Authorization for Treatment Purposes

Disclosures 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, or
- 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.

3.7 Routine Use and Disclosure of PHI

without Patient Authorization for Plan Operations Purposes

Disclosures for the BU Health Plans' Operations
Operations of the BU Health Plans includes all of the activities necessary to properly manage the BU Health Plans, such as:

- Quality assessment and improvement activities (but not generalized research),
- Compliance, risk management, auditing and legal services,
- Investigations of possible fraud and abuse,
- Business development and planning, or
- Other business and administrative activities required for the BU Health Plans to operate.

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

3.8 Routine Disclosures of PHI to Providers and Other Health Plans

Health care providers and health care plans may share information about the patients/participants who are common to both for payment purposes.

Minimum Necessary Rule applies.

Disclosures for Operations of Other Covered Entities
HIPAA allows a BU Health Plan 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 participant 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 BU Health Plans are encouraged to contact the BU HIPAA Privacy Officer for guidance.

3.9 Disclosing PHI to Business Associates

BU Health Plans may engage, or BU may engage on behalf of the BU Health Plans, entities outside of BU to perform various services. When the services involve the outside entity accessing, using, creating, or disclosing PHI held by any BU Health Plans, those entities are likely Business Associates of the BU Health Plans. The University, including its BU Health Plans, will 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, generally 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 BU Health Plans.

Responsibilities
The *Office of the General Counsel*, in consultation with the *BU HIPAA Privacy Officer* will:

- Approve a standard form Business Associate Agreement and make it available to the BU

Health Plans and Support Units; and
- Approve any changes to a Business Associate Agreement.

The *BU HIPAA Privacy Officer* will:

- Be available to advise BU Health Plans and Support Units on whether a service provider is a Business Associate; and
- Periodically audit the Business Associate logs and agreements maintained by BU Health Plans and Support Units.

The *BU Health Plans* 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 for approval of any change to the terms of the standard approved Business Associate Agreement; and
- Maintaining a log of all Business Associates and copies of all Business Associate Agreements for that BU Health Plan.

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 BU Health Plans 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 BU Health Plans Workforce;
- provides a service, or performs a function, or assists in the performance of a function or activity on behalf of a BU Health Plans; and
- in performing its duties for the BU Health Plans, 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.

Enforcement of Business Associate Agreements

If the BU Health Plans becomes aware of any material 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 that considers itself to be a Business Associate sends its own form of Business Associate Agreement to be signed, please inform the Business Associate that the PHI belongs to BU and its patients/participants 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 BU Policies and Procedures

- HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components
- HIPAA Policies for BU Health Plans *[current page]*
- 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 Health Plans