Effective Date: **August 1, 2013** Revised: **November 1, 2018**

POLICY

INFORMATION MANAGEMENT, RESEARCH AND SCHOLARLY ACTIVITIES

HIPAA Policies for Healthcare Providers at Covered Components: Policy 1, HIPAA Basics

RESPONSIBLE OFFICE

Research Compliance

This Policy 1 is part of the HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components.

1.1 HIPAA Covered Components

BU Covered Components

BU is a hybrid entity under HIPAA, meaning some of its operations are covered by HIPAA but many are not, and HIPAA allows BU to designate which of its components are HIPAA Covered Components. The following are the BU health care provider Covered Components:

1. Boston University Rehabilitation Services (including the BU Physical Therapy Center and BU Center for Neurorehabilitation),
2. Sargent Choice Nutrition Center,

3. Henry M. Goldman School of Dental Medicine Patient Treatment Centers, including the BU Dental Health Center,
4. The Albert and Jessie Danielsen Institute

Boston University Student Health Services fits the statutory definition of a Covered Component, but its records are either Education Records or Treatment Records under the Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g. As a result, Student Health Services is not subject to either the HIPAA Privacy Rule or the HIPAA Security Rule and is not subject to these policies.

Support Units

Each of the Covered Components receives services from a number of BU units that are not Covered Components. These are referred to as Support Units. BU Support Unit employees who use or disclose PHI in the course of providing services to any Covered Component have the same responsibilities to protect PHI as members of the Workforce of the Covered Component.

BU has identified the following units as Support Units whose services to Covered Components commonly use or disclose the Covered Component's PHI:

- Information Services & Technology, including Boston University Medical Campus Information Technology
- Financial Affairs, including Internal Audit and Advisory Services, Risk Management, and Accounts Payable
- Office of the General Counsel

Note: BU maintains many types of sensitive information not subject to HIPAA, such as student records whose confidentiality is governed by FERPA; patient records in units that do not conduct electronic transactions that make them subject to HIPAA but remain subject to state law; human resources records governed by federal and state law, and certain human subjects research data protected by federal and state laws. BU takes seriously its obligations under each of these laws and protects those records accordingly.

1.2 Key Roles

The HIPAA Privacy and Security Officers are your primary resources for HIPAA Compliance. You may reach them at the following e mail address: hipaa@bu.edu. Use that address to ask questions or to report a potential breach. Security incidents may be reported at irt@bu.edu, or by phone at 617-358-1100.

The BU HIPAA Security Officer is responsible for the development and implementation of policies to ensure compliance with HIPAA's Security Standards.

The BU HIPAA Privacy Officer is responsible for the development and implementation of policies to ensure compliance with HIPAA's Privacy Standards.

Covered Component HIPAA Contact:
Each Covered Component must designate one person to serve as the Covered Component HIPAA Contact, responsible for implementing these HIPAA policies in that Covered Component.

The BU HIPAA Privacy Officer and BU HIPAA Security Officer work closely with each Covered Component's HIPAA Contact on implementation of HIPAA compliance in their units and serve as key resources.

The persons serving in these key roles are listed in Appendix A.

1.3 What is PHI?

Protected Health Information (PHI) is any *individually identifiable health information* that can be linked to a particular person. It includes all information that was received, created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. This

information relates to:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual; or,
- The past, present, or future payment for the provision of health care to the individual.

What is not PHI?

Health information that does not identify an individual or that cannot be used to identify an individual is not PHI, but great rigor is required to confirm that no identifier is present in the dataset. For example, a data set of vital signs by themselves do not constitute PHI. However, if the vital signs data set includes medical record numbers, then the data set has not been successfully de-identified and must be protected as PHI.

Some types of health information are not subject to HIPAA, even if they clearly identify the individual:

- Research data that identifies an individual in research performed by an entity that is not subject to HIPAA,
- Information in treatment and education records covered by FERPA,
- Information in treatment records retained by BU health care provider units that are not designated as Covered Components,
- Health information in medical records about a person who has been deceased for more than 50 years,
- Information in BU's Human Resources employment records, and
- De-identified data, as described in Section 1.4: De-Identified PHI, below.

The types of information listed above are not subject to this Policy, but must be protected as set forth in the University's Data Protection Standards.

1.4 De-Identified PHI

If PHI is de-identified in the manner described below, the resulting data is no longer PHI and its use and disclosure will not be subject to HIPAA. Thus, no individual Authorization is needed to use the de-identified data.

There are two methods for de-identifying.

Removal of Identifiers Method
All of the following identifiers of the individual and of relatives, employers, or household members of the individual, are removed:

- (i) Names;
- (ii) All 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 if, according to the current publicly available data from the Bureau of the Census:
    - (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- (iii) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- (iv) Telephone numbers;
- (v) Fax numbers;
- (vi) Electronic mail addresses;
- (vii) Social security numbers;
- (viii) Medical record numbers;
- (ix) Health plan beneficiary numbers;
- (x) Account numbers;
- (xi) Certificate/license numbers;
- (xii) Vehicle identifiers and serial numbers, including license plate numbers;
- (xiii) Device identifiers and serial numbers;
- (xiv) Web Universal Resource Locators (URLs);
- (xv) Internet Protocol (IP) address numbers;
- (xvi) Biometric identifiers, including finger and voice prints;

- (xvii) Full face photographic images and any comparable images; and
- (xviii) Any other unique identifying number, characteristic, or code.

On rare occasions, even when PHI is de-identified, the individual can be identified. Typically, that occurs when the patient's condition and/or circumstances are very rare and/or may have been publicized. Thus, even when the 18 identifiers are removed, the Covered Component needs to confirm there is no reasonable basis to believe that the information could be used to identify an individual.

The BU HIPAA Privacy and Security Officers are available to confirm the information has been adequately de-identified, or to assist with obtaining the data in another form.

Expert Opinion Method

If a Workforce member believes the data s/he wishes to use cannot be linked to an individual, but it does not meet the criteria for "de-identified" (for example, dates of treatment are included), the Workforce member should contact the BU HIPAA Privacy Officer for assistance in obtaining an expert opinion that the risk is very small that information could be connected to an individual. There are specific requirements to be followed under HIPAA in using this method, and the HIPAA Privacy Officer can ensure the regulations are followed.

Re-Identifying De-Identified PHI

The Covered Component may, at its discretion, decode or translate de-identified PHI in order to re-identify the information with respect to specific individuals. The following requirements must be met:

- The re-identification process must be performed in a secure manner;
- The code, algorithm, table or other tool for re-identification may not be disclosed to any third-party or used for any purpose other than re-identification by the Covered Component; and
- The re-identification process utilized must be incapable of being translated or decoded by a third-party so as to identify the patient (e.g., the code cannot be a derivative of the patient's name).

1.5 The Covered Component's Designated Record Set

The Designated Record Set includes the Individual's medical records that are used, in whole or in part, by the Covered Component to make decisions about an Individual. Typically included are the provider's assessment and care of the Individual including diagnoses, diagnostic studies and tests, treatment, outcome, referrals, and disposition. The Designated Record Set also includes all billing records.

The Designated Record Set is important in fulfilling Individuals' rights under HIPAA. For example, when an Individual requests access to or a copy of his/her record, it is the Designated Record Set that is provided.

The Covered Component HIPAA Contact is responsible, with guidance from the BU HIPAA Privacy Officer, for determining and recording the Covered Component's Designated Record Set. Various portions of the Designated Record Set may be maintained in multiple locations within the Covered Component, and may include paper PHI, electronic PHI and other tangible PHI such as X rays, microfiche, photographs and audio recordings.

1.6 The Covered Component's HIPAA Workforce

The HIPAA Workforce consists of all faculty, employees, volunteers, health care providers, trainees (students participating in treatment), and other persons whose work is under the control of the HIPAA Covered Component, regardless of whether they are paid directly by a HIPAA Covered Component, whose work requires accessing, using, disclosing or creating PHI of that Covered Component.

Note: Students who do not participate in providing care and persons shadowing care providers are not members of the Workforce. See Section 5.6: Disclosures of PHI to Students and Observers.

Designation of Covered Component Workforce

The Covered Component's HIPAA Contact is responsible, with guidance from the BU HIPAA Privacy Officer, for designating and documenting who is in the Covered Component's HIPAA Workforce, and for updating the designation continually as needed.

Designation of the Covered Component Workforce is to be recorded by each Covered Component in the BU HIPAA SharePoint site, including each person's name, title, level of access to PHI, assigned training and completion of training.

1.7 Access to PHI

Levels of Access

The Covered Component HIPAA Contact is responsible for determining the level of access to PHI to be provided to each Workforce Member, and for documenting and monitoring that access level, with guidance from the BU HIPAA Privacy Officer and HIPAA Security Officer. Access must be role based; in other words, the level of access granted to each individual depends upon the type of PHI required by the Workforce member to carry out his/her duties. Health care providers should have unrestricted access to their patient records.

Termination of Access

The Covered Component HIPAA Contact is also responsible for ensuring access to PHI is terminated when a person is no longer a member of the Workforce due to termination of employment, reassignment to a position at BU outside the Covered Component, change in duties affecting need for access to PHI, retirement, extended leave (beyond 2 months) or any other reason. In addition, the HIPAA Contact needs to ensure the departing Workforce Member has not retained any BU PHI or other confidential BU data on devices or in any other form.

This includes immediately:

- terminating access to the premises by requiring the return of keys and badges,
- terminating electronic access to applications, systems or facilities, and
- ensuring departing Workforce members leave at BU any tangible PHI and remove any ePHI they may have received while in the Workforce from any device that they are not leaving with the Covered Component upon exiting.

Documentation and Local Auditing

Covered Component HIPAA Contacts are responsible for creating procedures that define how

access to ePHI is authorized, maintained, and revoked. Typically, this will consist of a matrix listing all Workforce members and their access rights.

See Policy 8 on access management.

1.8 HIPAA Training

All members of the Workforce of each BU Covered Component and Support Unit employees who support the Covered Components and who may have access to PHI are required to complete Boston University HIPAA training, as specified by the BU HIPAA Privacy Officer and the BU HIPAA Security Officer. This training will explain the privacy and security provisions of HIPAA as well as providing an overview of BU's HIPAA Privacy and Security policies. A new member of a Covered Component's Workforce or of a Support Unit shall complete training before having access to any PHI and all will complete refresher HIPAA training annually thereafter.

Responsibilities of Covered Components

The Covered Component HIPAA Contact must ensure training is completed as required by this Policy and must track and document the completion of training by each Workforce Member.

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, Protected Health Information - HIPAA for BU Healthcare, Research and Scholarly Activities, Research Compliance and Safety