Effective Date: **April 10, 2017**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

HIPAA Policies for BU Health Plans: Policy 1, Basics

RESPONSIBLE OFFICE

Research Compliance

This Policy 1 is part of the HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans.

1.1 HIPAA BU Health Plans

BU Health Plans

The following are the BU Health Plans that are Covered Entities subject to HIPAA and these BU Health Plan policies:

- Boston University Health Plan, Plan No. 502;
- Boston University Dental Health Plan, Plan No. 703; and
- Boston University Flexible Benefit Plan.

Support Units

Each of the BU Health Plans receives services from a number of BU units that are not BU

Health Plans (“Support Units”). BU employees of a Support Unit who use or disclose PHI in the course of providing services to any BU Health Plan have the same responsibilities to protect PHI as members of the Workforce of the BU Health Plans.

BU has identified the following units as Support Units whose services to BU Health Plans commonly use or disclose the BU Health Plans’ PHI:

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

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 protected by state law; human resources records governed by federal and state law; and most research data. 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 email 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.

BU Health Plans HIPAA Contact
The BU Health Plans HIPAA Contact is responsible for implementing these HIPAA policies in the BU Health Plans.

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

Support Unit HIPAA Contact:
Each Support Unit designates one person to serve as the Support Unit HIPAA Contact Person, responsible for implementing the privacy and security policies in that Support Unit. These Contacts will work closely with the BU HIPAA Privacy Officer and the BU HIPAA Security Officer on implementation of HIPAA compliance in their units.

A chart identifying the persons in these key roles is found 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 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, including BU Health Plan enrollment data.

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 itself does 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;
- Information in education records covered by FERPA;
- Information on insurance maintained by BU that are not Covered Entities under HIPAA, such as life insurance and disability insurance plans;
- 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 (with the exception of employee benefit records); and
- De-identified data, as described 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:

- Names;
- 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:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- 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;
- 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;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

On rare occasions, even when PHI is de-identified, the individual can still be identified. This occurs typically when the patient's condition and/or circumstances are very rare and have been publicized. Thus, even when the 18 identifiers are removed, the BU Health Plans need 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. As an alternative to de-identification by removing the 18 identifiers, data can be considered adequately de-identified if an expert provides an 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 BU Health Plans 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 BU Health Plans; 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 BU Health Plans’ Designated Record Set

The Designated Record Set includes the Individual’s records that are used, in whole or in part, by the BU Health Plans to make decisions about an Individual. All of the documents used in making decisions about an individual are included in the Plans’ Designated Record Set. Various portions of the Designated Record Set may be maintained in multiple locations within the BU Health Plans, and may include ePHI, paper PHI, and other tangible PHI.

1.6 The BU Health Plans' Plan Documents and Firewall

The Firewall
BU Health Plans will ensure that:

- Plan documents restrict Uses and Disclosures of PHI by BU consistent with HIPAA Privacy and Security Regulations;
- Procedures are established for preventing the improper Uses and Disclosures of PHI by BU;
- Administrative, physical, and technical safeguards are implemented that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that BU creates, receives, maintains, or transmits on behalf of BU Health Plans; and
- The employees of BU who have access to BU Health Plans' PHI are identified by name or by job function (See Appendix B, BU Health Plans HIPAA Firewall Listing).

Designation of BU Health Plans Workforce within the Firewall
The BU Health Plans' HIPAA Contact is responsible, with guidance from the BU HIPAA Privacy Officer, for designating and documenting who is in the BU Health Plans' HIPAA Workforce within the Firewall, and for updating the designation continually as needed.

1.7 Access to PHI

Levels of Access
The BU Health Plans 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.

Termination of Access
The BU Health Plans 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 BU Health Plans, change in duties affecting need for access to PHI, retirement, or any other reason. In addition, the HIPAA Contact needs to ensure the departing Workforce member has not retained any BU Health Plans PHI or other confidential BU Health Plans 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 remove any ePHI they may have received while in the Workforce from any device that they are not leaving with the BU Health Plans upon exiting.

Documentation and Local Auditing
BU Health Plans HIPAA Contacts are responsible for creating procedures that define how access to ePHI is authorized, maintained, and revoked.

The BU Health Plans HIPAA Contact must create an auditable process for initial granting of access and changes to access rights when the Workforce Member's role and PHI access has changed, and they must conduct a self-audit quarterly.

See Section 8.2.3.2 Provisioning and Deprovisioning of Accounts and Authorizations and the University's Identity and Access Management Policy.

1.8 HIPAA Training

All members of the Workforce of each BU BU Health Plan 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. Each Workforce member shall complete refresher HIPAA training annually thereafter.

A new member of a BU Health Plans' Workforce shall complete training before having access

to any PHI.

The BU Health Plans 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. If tracking and documentation is provided by a BU learning management system, the HIPAA Contact shall audit the records of that system quarterly.

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 -