Effective Date: **April 10, 2017**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

HIPAA Policies for BU Health Plans: Policy 2: Individual Responsibilities for Safeguarding PHI

RESPONSIBLE OFFICE

Research Compliance

This Policy 2 is part of the HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans.

2.1 Safeguarding Paper and other Tangible PHI

BU Health Plans Workforce members who use or disclose PHI are responsible for taking appropriate precautions to prevent unauthorized access to PHI during the course of daily operations including:

- Do not remove paper or tangible PHI unless approved by the HIPAA Contact.
- If you are allowed to remove PHI, do not leave it, or any file, box, briefcase or portable electronic device containing PHI, anywhere they can be easily stolen, such as cars.

- Avoid displaying or storing PHI in predominantly public spaces or in spaces that visitors must pass through to access other parts of the facility.
- Report any suspicious activity, including apparent physical maintenance that seems inappropriate or unscheduled.
- Do not leave PHI on desks when not working on it. Safely store PHI even if you step away from your desk or work area just for a minute.
- Lock all PHI away at night in a cabinet or locked office.
- Never dispose of paper or other tangible PHI in the trash. Use a cross-cut shredder.
- Do not store PHI in a “shred box” under your desk. It’s too easy to confuse it with trash.
- Off-site storage of paper records may be used, provided the storage company offers appropriately secure conditions and signs a Business Associate Agreement.
- Transmitting paper or other tangible PHI by US Mail or other reliable delivery services such as UPS, FedEx and DHL is permissible, but use common sense in not overstuffing envelopes and using appropriate boxes and envelopes to minimize the possibility of loss in transit.
- Transmitting paper PHI via facsimile is permissible. Please program frequently used numbers into the fax machine, and confirm you are faxing to the correct number.

2.2 Safeguarding Verbal PHI

Conversations

Do not discuss BU Health Plans information regarding participants and other sensitive information in public areas, such as the waiting room, cafeteria, restaurant, street, elevator, stairwell or any place else. You may think you are masking the individual’s identify by not using a name or telling all of the details, but it is still inappropriate and risks a HIPAA breach.

PHI on the Telephone

Landlines and mobile phones are reasonably secure and may be used to communicate PHI. Callers should still use common sense precautions:

- Ensure no one in the vicinity can overhear what is said;
- Avoid use of a speaker phone if unauthorized persons could hear the conversation; and
- When leaving a voice mail for an Individual, leave the minimum necessary information unless the participant has authorized you in writing to leave substantive messages. A

minimum necessary voice mail would be something like, “This voice mail is for [participant name]. This is [your name] at the [BU Health Plans name]. Please return my call at 617-xxx-xxxx.”

2.3 Safeguarding Electronic PHI

1. Only use electronic devices that are approved for use by the BU Health Plans.
2. Only store ePHI on devices approved by the BU Health Plans.
3. Only share ePHI using applications and storage locations approved by the BU Health Plans
4. If a BU Health Plans’ procedures allows its Workforce members to access ePHI from a personal device, Workforce members must ensure devices are kept in compliance with all aspects of the Security Rule as defined in Section 8.
5. When sending ePHI via e-mail:
    1. Ensure the recipient is authorized to have access to the ePHI
    2. Use encryption such as:
        1. An approved e-mail communication tool (DataMotion);
        2. Encrypt the document or spreadsheet before sending. If you choose to encrypt the document and send it via non-secure e-mail, take care to avoid identifying the patient in the subject line or body of the e-mail.
6. Do not send ePHI via text message
7. Do not position monitors displaying ePHI where they can be viewed by anyone outside the BU Health Plans’ “Firewall Workforce” – the workforce who are allowed access to the sensitive information held by the Health Plan, including PHI and ePHI.
8. Use PHI only with applications and systems approved by your HIPAA Contact.
9. Protect accounts, passwords, and workstations:
    1. Create and periodically change passwords that conform to best practices for selecting passwords, even if not enforced or required by the system.
    2. Immediately change your password and notify Information Security if there is reason to believe that a password has been improperly disclosed, accessed or used by an unauthorized person
    3. Do not share passwords related to any University system with any other person.
    4. Do not use University passwords for any non-University accounts.
    5. Only use administrator accounts with privileges as authorized and when necessary.

10. Only use encrypted removable media (CD-ROMs, DVDs, USB keys, tapes, etc.) for storing ePHI. See also Removable Media and Media Inventory.
11. Avoid duplicative storage of ePHI on devices by securely deleting or removing any unnecessary electronic copies.
12. Report to your HIPAA Contact or Information Security any unusual system activity including:
    1. Alerts displayed by a system or application indicating a problem
    2. Unusual behavior such as seeming loss of control of mouse or keyboard
    3. Alerts displayed by security software meant to prevent malicious code, such as antivirus
13. Report to your HIPAA Contact or Information Security potential security events such as:
    1. The loss of a device (personal or university-owned) that contains or has access to ePHI;
    2. The loss of a secondary authentication token, such as SecurID or Duo;
    3. Unusual account activity such as a last-login event occurring at an unusual time; or
    4. Someone accessing PHI who is not authorized to do so.
14. ePHI must be disposed of properly, according to Information Security's Media Destruction One Sheet. This means:
    1. Files on a computer system should be securely deleted.
    2. Media must be physically destroyed when no longer needed.
15. Only transmit or receive ePHI data when:
    1. Using Boston University's wired or wireless network,
    2. Using an encrypted communication protocol, such as secure e-mail (DataMotion), https, ssh, sftp, remote desktop, etc., or
    3. After establishing a connection via the Virtual Private Network (VPN) service.

Photographs, Audio and Video Recordings

Most photos, audio recordings and video recordings of patients are stored electronically. Use the same safeguards as for any electronic PHI.

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; Manual is also available as a PDF File, 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, www.bu.edu/hipaa
  - 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