Effective Date: **August 1, 2013** Revised: **September 20, 2024**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY, RESEARCH AND SCHOLARLY ACTIVITIES

HIPAA Policies for Healthcare Providers at Covered Components: Policy 2, Individual Responsibilities for Safeguarding PHI

RESPONSIBLE OFFICE

Research Compliance

This Policy 2 is part of the HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components.

2.1 Safeguarding Paper and other Tangible PHI

Unlike Section 8, which outlines how the BU HIPAA Security Program must be executed, the three sections of Policy 2 outline how individual workforce members must protect tangible, verbal, and electronic PHI from unauthorized access during the course of daily operations. For example:

- Do not remove paper or tangible PHI (e.g., x-ray or photo) from a Covered Component

unless approved by the HIPAA Contact;
- If you are allowed to remove PHI, do not leave it, where it can be easily stolen, such as the back seat of an automobile;
- Avoid displaying or storing PHI in public spaces or hallways;
- Report any suspicious activity, such as unscheduled maintenance;
- 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, and when not working on it, in a cabinet or locked office;
- If a Covered Component facility is visible from the exterior, close window blinds to prevent outside disclosure, or confirm patients are comfortable;
- Never dispose of paper or other tangible PHI in the trash. Use a secure destruction method, such as cross-cut shredder;
- Do not store a “shred box” under your desk. It’s too easy for cleaning staff to confuse it with trash and dispose of it in a non-secure manner;
- Sending paper or other tangible PHI by fax, mail, or reliable delivery services is permissible, but please double check destination addresses and use appropriate boxes and envelopes;

2.2 Safeguarding Verbal PHI

Conversations

Do not discuss patients in a public areas such as the waiting room or elevator.

Waiting Room Configuration

Arrange the waiting areas in such a way as to minimize one patient overhearing conversations with another. Useful approaches include:

- Posting a sign to keep patients waiting in line back from reception conversation,
- and/or playing ambient music or white noise to cover reception conversation.

PHI on the Telephone

Landlines and mobile phones are reasonably secure for having conversations.

Take precautions to ensure no one in the vicinity can overhear conversations (e.g., shut office doors, use sound machines). If patients or research subjects leave you voicemail messages,

it is a best practice to include language in your voicemail message discouraging them from including sensitive information. Likewise, when you are leaving voicemail messages, remember to avoid disclosing any sensitive information. For example:
“This voice mail is for [patient name]. This is [your name] at the [Covered Component name]. Please return my call at 617-xxx-xxxx.”

2.3 Safeguarding Electronic (ePHI)

1. Only use devices, applications, services, and storage approved by the Covered Component. BU IS&T HIPAA compliant applications are listed here and storage options are listed here.
2. Never use personal desktops, laptops, or tablets for accessing, processing, or storing ePHI. For any Covered Component that wants to take on the risk of permitting personal desktops, laptops, or tablets, they must submit an Application for Exception to BU HIPAA Policies outlining how they will: (1) verify student computers meet the BU Minimum Security Standards, (2) document the verification, and (3) verify removal of ePHI from personal desktops, laptops, and tablets before removing them from the Covered Components Inventory.
3. BU Microsoft apps can be used on a personal phone if
    1. Encryption and screen lock are enabled, typically by requiring a password, passcode, or biometric for logging into the device.
    2. Cloud sync to Apple or Google or any other service besides BU Microsoft HIPAA compliant apps is disabled, and
    3. A factory reset is conducted before letting any person or entity have access to the phone. For example, a factory reset must be conducted before trading a phone in for an upgrade or giving the phone to a family member.
4. Never turn on auto-forwarding of BU email to non-BU email systems. For example, the emails you receive at your name@bu.edu address cannot be auto-forwarded to your email address outside of BU, such as name@gmail.com, name@apple.com, or name@yahoo.com.
5. In general, email is not a secure method for sending ePHI. While it is permitted to send scheduling information – such as BU Teams or Zoom meeting links, appointment options and reminders – information about a patient’s condition or treatment can never be sent by BU Outlook, except as outlined below:

a. Ensure the recipient is authorized to have access to the ePHI.
b. Never use Gmail or other Google apps.

6. Share files containing ePHI directly from BU Microsoft Teams, SharePoint, or OneDrive; Microsoft will send an email to the recipient with a link to the file. Alternatively, copy the link to the file from the Microsoft location and add the link to a BU Outlook email for the recipient.
   a. Use approved email communication tool (DataMotion).
   b. Use a HIPAA Compliant BU Outlook Account, that has several extra controls, including automatic deletion of emails that are 365 days old. Regular BU Outlook accounts cannot be used.
7. Do not send ePHI via regular SMS text message:
   a. You may send de-identified patient information to co-workers in a text message, for example, “your 2:00 appoint called to cancel” or “can we meet at noon tomorrow to discuss our new patient with Parkinson’s?”
   b. Use BU Teams or Zoom chat function to send ePHI securely to co-workers or patients.
   c. Use a secure text messaging app, such as BU REDCap with the Twilio secure text service.
8. Do not position monitors displaying ePHI where they can be viewed by the public (e.g., patient hallway).
9. Protect accounts and passwords:
   a. Create and periodically change passwords that conform to best practices for selecting passwords even when not enforced by the system;
   b. 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;
   c. Do not share passwords;
   d. Do not use University passwords for any non-University accounts; and
   e. Only use administrator accounts with privileges as authorized and when necessary.
10. In general, portable media is blocked on BU managed desktops, laptops, and tablets at BU HIPAA Components, to lower the risk of malicious software infection. If you are using a computer that has an exception, only use external media (e.g., CD, USB thumb drive) that is approved and inventoried by the HIPAA Contact.
11. Report to your HIPAA Contact and/or ithelp@bu.edu for potential security events such as:
    a. The loss of a device (personal or university-owned) that contains or has access to

ePHI;

b. Unusual behavior, such as seeming loss of control of mouse or security software (e.g., Crowdstrike) alert;

c. Unusual account activity such as a last-login event occurring at an unusual time; or

d. Someone accessing ePHI that is not authorized to do so.

12. Only transmit or receive ePHI data when:

a. On-campus, using Boston University's wired or wireless network; or

b. Off-campus, using a Boston University two-factor VPN

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