Effective Date: **August 1, 2013** Revised: **October 13, 2020**

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

Office of 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 may 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 PHI

1. Only use devices, applications, services, and storage approved by the Covered Component.
2. If a Covered Component's procedures allow its Workforce Members to access ePHI from a personal device, they must complete a Security Attestation as part of annual training, and before any new devices are used to access ePHI. Workforce members must also remove PHI, ideally with a factory reset, before their control of the device ends (e.g., sale or trade-in).
3. When sending ePHI via email:
    1. Ensure the recipient is authorized to have access to the ePHI;
    2. Use encryption such as:
        1. an approved email communication tool (DataMotion);
        2. Encrypt the document or spreadsheet before sending. See Microsoft Support Article. If you choose to encrypt the document and send it via non-secure email, take care to avoid identifying the patient in the subject line or body of the email.
    3. If a patient requests use of non-secure email, follow Section 6.6: Right to Request Confidential and Alternate Modes of Communications that addresses non-secure email Requests.
4. Do not send PHI via text message:
    1. 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?"

2. If a patient requests use of text messaging, follow Section 6.6: Right to Request Confidential and Alternate Modes of Communications that addresses non-secure email/text requests.

5. Do not position monitors displaying ePHI where they can be viewed by the public (e.g., patient hallway).
6. Protect accounts abd passwords:
    1. Create and periodically change passwords that conform to best practices for selecting passwords even when not enforced 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;
    4. Do not use University passwords for any non-University accounts; and
    5. Only use administrator accounts with privileges as authorized and when necessary.
    6. Any external media (e.g., CD, USB thumb drive) must be encrypted and inventoried by the HIPAA Contact.
7. Avoid duplicative storage of ePHI on devices by securely deleting or removing any unnecessary electronic copies. And when devices reach end of life, the hard drive must be destroyed, even when data on the hard drive is encryted. BU provides shredding of media at not cost to BU faculty, staff, and students. Contact IS&T for pickup or dropoff options.
8. 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. Unusual behavior, such as seeming loss of control of mouse or security software (e.g., Crowdstrike) alert;
    3. Unusual account activity such as a last-login event occurring at an unusual time; or
    4. Someone accessing PHI that is not authorized to do so.
9. Only transmit or receive ePHI data when:
    1. On-campus, using Boston University's wired or wireless network; or when off-

campus, 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