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

Anyone who uses or discloses PHI is responsible for taking appropriate precautions to prevent unauthorized physical access to it during the course of daily operations. For example:

- Do not remove paper or tangible PHI from a Covered Component 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 it, anywhere they can be easily stolen, such as cars;
- Avoid displaying or storing PHI in 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 to a Covered Component’s facility 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;
- If a Covered Component facility is visible from the exterior, close window blinds to prevent outside disclosure;
- Never dispose of paper or other tangible PHI in the trash. Use a 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;
- 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 reliable delivery services such as UPS, FedEx and DHL is permissible, but use common sense in not overstuffing envelopes, and use 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 patients in a public area such as the waiting room, cafeteria, restaurant, street, elevator, stairwell or any place else. You may think you are masking the patient’s identify by not using a name or telling all of the details, but someone who overhears may recognize the person; in any event, such conversations reflect poorly on us and even if deidentified, are still inappropriate.
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, or
- Ambient music or white noise to cover reception conversation.

**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, such as ensuring no one in the vicinity can overhear what is said.
- Avoid use of a speaker phone if unauthorized persons could hear the conversation.
- When leaving a voice mail for an Individual, leave the minimum necessary information unless the patient has authorized you in writing to leave substantive messages. A minimum necessary voice mail would be something like, “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 electronic devices that are approved for use by the Covered Component in its procedures.
2. Only store ePHI on devices approved by the Covered Component.
3. Only share ePHI using applications and storage locations approved by the Covered Component.
4. If a Covered Component’s procedures allow its Workforce Members to access ePHI from a personal device, those personal devices must meet the standards set in **Policy 8, HIPAA Security Program**, including encryption; password protection; anti-malware and other such measures described in Policy 8.
5. 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](http://www.bu.edu/policies/hipaa-indiv-responsibilities-safeguarding-phi/)).
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.

6. 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.

7. Do not position monitors displaying ePHI where they can be viewed by the public.

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 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 related to any University system with any other person;
   4. Do not use University passwords for any non-University accounts; and
   5. Only use administrator accounts with privileges as authorized and when necessary.

10. Your Covered Component procedures will state whether it is permissible to use removable media (CD-ROMs, DVDs, USB keys, tapes, etc.) for storing ePHI.

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; or
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 that is not authorized to do so.

14. Media and devices containing 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, and
    2. Media must be physically destroyed by BU IS&T 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 email (DataMotion), https, ssh, sftp, remote desktop, etc.; or
    3. After establishing a connection to via the Virtual Private Network (VPN)

Photographs, Audio and Video Recording of Patients
Most photos, audio recordings and video recordings of patients are stored electronically. Use the same safeguards as for any electronic PHI. When they are in a tangible form (e.g., a printout, x-ray or a photograph) follow the precautions listed above for Paper and Other Tangible PHI.

__________________________
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