Effective Date: **April 10, 2017** Revised: **March 11, 2025**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

HIPAA Policies for BU Health Plans: Policy 7, Breaches

RESPONSIBLE OFFICE

Research Compliance

This Policy 7 is part of the HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans.

7.1 Obligation to Report Potential Breaches

Any Workforce member who learns that a potential breach of PHI may have occurred, s/he must immediately notify his or her supervisor and/or the BU Health Plans' HIPAA Contact. The HIPAA Contact shall ensure the report is forwarded immediately to the BU HIPAA Privacy Officer. Reports may be sent to the BU HIPAA Privacy Officer at hipaa@bu.edu.

If the potential breach relates to electronic information, the Workforce member must also notify the BU Information Security Incident Response Team at irt@bu.edu or 617-358-1100

Failure to make a report in circumstances where the Workforce member is required to do so may lead to discipline, up to and including termination of employment.

7.2 Obligation to Mitigate Potential Breaches

If a Workforce member within the firewall becomes aware of an inadvertent misuse or wrongful Disclosure of PHI, the employee, on his/her own or seeking assistance of others within the firewall, will take reasonable measures to end or limit the misuse.

If, according to the particular circumstances of the misuse or wrongful Disclosure, it is reasonable to do so, the HIPAA Privacy Officer or Designee may be asked to evaluate the specific situation and determine if any further corrective action is needed.

If a Business Associate's practices or patterns of activity have violated the privacy regulations, an employee within the firewall or HIPAA Privacy Officer will take reasonable steps to cure the violation. If such steps are unsuccessful, the contract may be terminated and steps taken to report Security Incidents or Breaches of Unsecured PHI in accordance with HIPAA and these policies and procedures.

If an internal function within BU violates the privacy regulations, appropriate steps including Breach notification, outreach to the plan participants involved, application of Sanctions, retraining, etc. will be determined by the HIPAA Privacy Officer.

The BU Health Plans will mitigate, to the extent practicable, any harmful effect known from unauthorized Use or Disclosure of PHI in violation of the HIPAA Privacy regulation.

Examples of unauthorized Use or Disclosure of PHI by BU Health Plans:

- An employee within the firewall receives a claims data report from a Business Associate and forwards to an employee within the firewall for review and analysis. The report is accidentally sent to the wrong person via e-mail or interoffice mail. Once the error has been detected, the employee within the firewall shall take reasonable steps to retrieve the file from the person who received it. As a reasonable precaution against this contingency, employees who handle e-mails, files or reports containing PHI electronically

could establish an address book specifically listing others within the firewall.

- BU Health Plans become aware of an electronic breach of its corporate firewall, either intentional or unintentional. In such a case, BU internal Information Technology specialists may be required to evaluate whether specific data may have been improperly accessed. If such data is determined to have contained ePHI, the Group Health Plan will use all reasonable efforts to see that the ePHI is reobtained and/or destroyed and may, in accordance with HIPAA's breach notification rules, also take steps to identify and notify the Individual(s) who were the subject(s) of such ePHI about the breach.
- BU Health Plans become aware that Business Associate discusses PHI with persons not on the list of employees within the firewall (i.e., discussing a participant's claim with a supervisor or colleague). BU Health Plans will contact the Business Associate and take reasonable steps to cure the violation, including verifying that that Business Associate is utilizing the proper list of employees within the firewall.
- BU Health Plans become aware that a Business Associate is sharing or selling participant names and/or diagnoses to a pharmaceutical company. BU Health Plans will contact the Business Associate and take reasonable steps to cure the violation, terminate the contract and as required under HIPAA's breach notification rules, notify affected individuals and HHS.
- BU Health Plans become aware that a Business Associate has mailed ID cards or other documentation containing PHI: (i) to the wrong participant; or (ii) in such a way that PHI is visible through the envelope window. BU Health Plans will contact the Business Associate and require it to take reasonable steps to correct the mailing, including identifying and contacting all Individuals who may have had PHI inadvertently disclosed in this manner in accordance with HIPAA's breach notification rules.

7.3 No Retaliation

Neither the BU Health Plans nor anyone else affiliated with BU may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for his/her exercise of any right established by, or for participation in any process provided for, these policies or the law, including:

- Filing a complaint with the BU Health Plans;
- Filing a complaint with governmental authorities;
- Assisting or participating in an investigation or compliance review by BU or its agents;

- Testifying in a proceeding or hearing by governmental authorities under HIPAA; or
- Opposing any act or practice made unlawful by HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve an impermissible disclosure of PHI.

Individuals who report breaches may be subject to the protections of the University's Code of Ethical Conduct.

7.4 Response to Reports of Potential Breaches: Investigation and Remedial Action

Responsibility to Receive, Record and Investigate Reports
BU's HIPAA Privacy Officer and HIPAA Security Officer will:

- Receive and respond to all notifications of the use or disclosure of PHI in violation of these Policies or of HIPAA;
- Record all reports of potential breaches;
- Investigate each according to the university's Data Breach Management Plan to determine whether the circumstance constitute a breach; and
- Document the conclusion.

In investigating electronic incidents the HIPAA Security Officer or HIPAA Contact should follow Information Security's First Responder Checklist to ensure that critical evidence is preserved. In addition, any Workforce member should take reasonable precautions against physical threats to information, such as closing a door found open, locking cabinets and doors and similar steps.

Confidentiality
BU will make all reasonable efforts to protect the confidentiality of persons reporting violations of law or of BU HIPAA policies or procedures, if requested, to the extent practicable, given the nature of the investigation.

Response to Breach

If PHI has been used or disclosed in violation of BU policy or HIPAA requirements, BU will mitigate, to the extent practicable, any known harmful effects. Examples of actions that will be taken, depending on the circumstances, include the following:

- If the violation involves a continuing unauthorized disclosure of PHI, steps will be taken to end the practice immediately;
- If the violation involves an unlawful activity or practice, the activity or practice will be stopped and the Office of the General Counsel will be notified of the violation; or
- If the same or a similar violation could or might be prevented in the future by making changes to HIPAA policies and procedures, training or guidance, such changes will be instituted and promptly communicated to all affected employees.

7.5 Breach Notifications

In the event the BU HIPAA Privacy and/or Security Officer determines a Breach has occurred, it will notify the affected individuals, the media and the Secretary, as applicable and as required under HIPAA, and will take appropriate remedial actions.

7.6 Enforcements and Sanctions

Members of the Workforce, who are determined to have violated any policy in the HIPAA Policy Manual or a Covered Component's policies or procedures, may be subject to disciplinary action, up to and including, termination of employment.

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 - HIPAA for BU Health Plans