Effective Date: **April 10, 2017**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

HIPAA Policies for BU Health Plans: Policy 8, Security Policy

RESPONSIBLE OFFICE

Research Compliance

This Policy 8 is part of the HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans.

This Security Policy governs PHI of the BU Health Plans.

Regardless of where or in what form (paper, electronic or otherwise) University data is stored, it remains the property of the University and the University's HIPAA BU Health Plans are responsible for ensuring proper protection.

The BU Health Plans must ensure the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) through the designation, creation, and maintenance of administrative, physical and technical controls. This HIPAA Security Program includes required policy and steps to assist the BU Health Plans in defining, documenting and maintaining security controls. Through the implementation of this Policy, BU Health Plans procedures and controls, BU Health Plans will help ensure the protection of the ePHI that they create, maintain, receive, and transmit.

Roles and Responsibilities

Management of the BU Health Plans are responsible for ensuring their operations comply with HIPAA, including this Security Policy. The compliance effort will be led by a designated HIPAA Contact within each BU Health Plan. Where compliance functions and controls can be run centrally they have been made the responsibility of the HIPAA Security Officer but some controls require local knowledge and involvement in day-to-day operations.

The HIPAA Security Officer will actively guide the compliance effort and IT support units will perform a portion of the work required for compliance.

Workforce members responsibilities under HIPAA are addressed in the HIPAA Privacy Policy in Section 2: Individual Responsibilities. Workforce members do not need to concern themselves with the details of this Security Policy unless they use a Personal Devices to use or store ePHI.

Security Program Structure

Boston University uses the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to define the HIPAA security program. The CSF identifies the key, ongoing steps as: Identify, Protect, Detect, Respond, and Recover. Our program integrates the HIPAA Security Rule requirements into the CSF, which requires ongoing movement through the phases to update understanding of cybersecurity risks. This section is organized according to these five phases.

Security Program Structure 5 Phases

Image not found or type unknown

The approach to compliance must be tailored to the risks of the BU Health Plans. Controls should be put in place that address security risks but are not so onerous or complex that they prevent the timely delivery of health services or so expensive that they impede operations. This HIPAA Security Policy is the basis of compliance for the BU Health Plans. The BU Health Plans will develop procedures to implement the program with the guidance and assistance of the BU HIPAA Security Officer. In many areas, BU has University-wide policies, including but not limited to the Information Security Policy and the Data Protection Standards. These are referenced and linked throughout this document to facilitate the development of BU Health Plans procedures consistent with these policies. The BU Health Plans may expand upon this program if desired provided that expansions are consistent with this document and all other University policies.

8.1 Phase 1: Identify

The first step of our security program is to identify the assets to be protected and the threats and vulnerabilities the assets need to be protected from. The basic steps included in this phase are:

1. Build a System and Application Inventory (Section 8.1.1)
2. Conduct a Security Risk Section 8.2 Assessment (Section 8.1.2)
3. Conduct Periodic Technical and Non-Technical Evaluations (Section 8.1.3)
4. Address security requirements for Business Associates (Section 8.1.4)

8.1.1 System and Application Inventory

The HIPAA Contact is responsible for ensuring the existence and maintenance of an inventory of all assets that contain ePHI including:

- Name for the asset, be it the name of the application, laptop, or server hostname;
- Description or identifier for each asset, such as a serial number, hardware specification or an application name;
- Classification, including ownership information. Classifications may include the device type and may be grouped (“workstation”, e.g.) when a repeatable design is used. If groups are used, the number of systems within a classification should be recorded;
- Normal location for a physical asset or class of assets, if applicable;
- Date the device was last cleared for use with HIPAA data and by whom; and
- Who the system or application administrators for the asset are.

The inventory is more than just a list of systems and applications associated with ePHI. It also assesses the relative importance of the assets to health care operations. A complete inventory also documents the:

- Dependency of key applications on the internal or external systems they are running on;
- Dependency of key systems on support technologies including University services such as the network, firewalls, virtual server environment, or similar services;
- Impact of the loss of an application or system related to the provision of care
- Priority score derived from the statement of impact; and
- Alternative solutions that may be employed if the application or system is unavailable.

The inventory describes the business impact of the unavailability of a physical location, data center, system, network, or application, what measures might be taken to compensate, and given the loss of multiple assets, where priority should be placed for restoration of normal service.

keys_infosec

Image not found or type unknown ***The HIPAA Contact is responsible for ensuring the inventory is updated any time there is a change in equipment, software, dependencies, or the IT priorities of the BU Health Plans.***

8.1.2 Security Risk Assessment

The HIPAA Security Officer, working with the HIPAA Contacts, Information Security, and Internal Audit & Advisory Services shall periodically conduct a comprehensive Security Risk Assessment that documents and prioritizes all reasonably anticipated, high-level administrative, physical, and technical risks to the confidentiality, integrity, and availability of ePHI. BU Health Plans and their Workforces are responsible for assisting with these comprehensive risk assessments.

keys_infosec

Image not found or type unknown ***The Security Risk Assessment identifies threats, vulnerabilities, risks, and controls. It does not assess the compliance of a BU Health Plans with this Policy.***

A Security Risk Assessment includes:

- A defined scope that includes all systems that create, receive, maintain, or transmit ePHI. This is normally completed as part of the System and Application Inventory.
- A list of threats to and vulnerabilities of those systems. This should be a high level classification of risk such as “Unavailability of electronic medical record (EMR) system due to component loss or failure” or “System Compromise leading to breach of ePHI” rather than a specific technical vulnerability. It should be narrow enough to define a security control to mitigate the risks but not so narrow to require an extensive list.
- An assessment of the existing countermeasures to mitigate those threats and vulnerabilities

- An assessment of the likelihood the vulnerabilities will be exploited by a threat.
- As assessment of the potential impact of such exploitation on the confidentiality, integrity, and availability of ePHI.

These four factors (i.e., threats, vulnerabilities, likelihoods, and impacts to ePHI) should be evaluated to create an overall rating for each risk and identify areas where security controls are lacking. After completing the assessment, the HIPAA Security Officer and HIPAA Contacts meet to review the findings and identify what security controls are appropriate to address their specific risks.

Risks are seldom perfectly addressed as doing so would either exhaust resources (staff, time, money, or all three) or render the asset unusable. The degree of mitigation for each risk requires the input of the BU Health Plans' management and the HIPAA Security Officer to identify the degree of acceptable risk.

The Security Risk Assessment must be reviewed annually by the HIPAA Security Officer and the BU Health Plans.

8.1.3 Periodic Technical and Non-Technical Security Review

The HIPAA Security Officer shall conduct periodic technical and non-technical reviews of the BU Health Plans' adherence to the requirements of this Policy. These should occur at least annually.

keys_infosec

Image not found or type unknown

The Security Review is an assessment of the BU Health Plans' compliance with this Policy, not a review of risks, though new risks may be identified during the process.

These reviews can include assessing whether the physical, technical, and administrative controls meet the requirements of this Policy, inspecting configurations on systems, conducting vulnerability scanning or penetration testing, auditing of documentation, or walking around a facility and checking doors, looking at how devices are physically secured, verifying alarm and video systems are functioning, and auditing other aspects of the physical controls. These reviews can also include Business Associate (BA) practices, especially exchanges of ePHI with Business Associates.

Findings shall be documented and may require a management response. A summary of such reviews shall be made accessible to the Information Security and Business Continuity Governance Committee and others as deemed appropriate to a particular review.

In addition, the BU Health Plans must initiate a review in response to changes in the environment, operational procedure, or significant changes in the risks to ePHI. These reviews may have a smaller scope, such as the planned acquisition of a new software package or physical relocation

8.1.4 Security Requirements for Business Associates

The HIPAA Security Rule also applies to Business Associates: non-BU persons or entities that provide services to the BU Health Plans requiring the access, use, creation or disclosure of PHI. Business Associates are not permitted access to PHI before signing a Business Associate Agreement (BAA). By signing a BAA), a Business Associate agrees to follow the requirements of the HIPAA Security Rule. Only use a BAA approved by the HIPAA Privacy Officer. See the HIPAA Privacy Policy at Section 3.9: Disclosing PHI to Business Associates.

The BU Health Plans remains responsible for determining appropriate access of the Business Associate, and for transmitting any PHI to the Business Associate securely, and terminating access when no longer needed. In addition, the University may have other obligations such as maintaining access controls and auditing access.

8.2 Phase 2: Protect

Once a set of risks are identified, the next step is the deployment of controls to mitigate those risks. The components of this phase are:
Specify Individual Responsibilities (Section 8.2.1)
Assess risks and designate required security controls (Section 8.2.2)
Deploy Administrative Controls (Section 8.2.3)
Deploy Technical Controls (Section 8.2.4)

Deploy Physical Controls (Section 8.2.5)

8.2.1 Individual Responsibilities

A key aspect of any security program is individual responsibility. Effective security relies on everyone doing their part to help maintain the security of our records, and a section of this document is focused on Individual Responsibilities. The education necessary to perform the tasks associated with these responsibilities will come from the Security Awareness training discussed later.

8.2.2 Risk Management through Security Controls

BU Health Plans must implement Security Controls sufficient to reduce risks and vulnerabilities. The HIPAA Contact should work collaboratively with the HIPAA Security Officer to:

- Prioritize the risks identified in the Security Risk Assessment and vulnerabilities found in Technical and Non-Technical Security Reviews.
- Create a remediation plan through the application of security controls.
- Specify, implement, validate, and audit the functioning of security controls.

keys_infosec

Image not found or type unknown

To meet compliance requirements, University level controls must be supplemented by controls specific to the BU Health Plans.

Controls are considered to have one of three forms: Administrative, Technical, or Physical, though some controls are hard to fit uniquely in one category.

8.2.3 Administrative Controls

Administrative controls include non-technical actions and policies to enforce security requirements, such as training.

8.2.3.1 Security Training and Reminders

Training
The BU HIPAA Security Officer shall provide a security training program for BU Health Plans. See the HIPAA Privacy Policy at Section 1.8: HIPAA Training.

Reminders
The HIPAA Security Officer will issue reminders and updates about security issues of critical concern. BU Health Plans must ensure these reminders reach all members of the BU Health Plans Workforce.

In addition, BU Health Plans are encouraged to provide additional reminders about security topics through the use of bulletin boards, newsletters, e-mail, staff meetings, or custom screensavers. The HIPAA Privacy Officer, HIPAA Security Officer, and Information Security are available to assist with ideas for important topics.

8.2.3.2 Provisioning and Deprovisioning of Accounts and Authorizations

BU Health Plans must create procedures that define how access to ePHI is authorized, maintained, and revoked, including:

- Creating a matrix of what access rights are required based on the role of the Workforce member.
- Creating an auditable process by which changes to access rights to ePHI (provision, alteration, or removal) are requested, approved, and completed including:
  - The request and its associated authorizations;
  - Where possible, an audit log of the change itself within the system or application.
- Documenting a procedure by which access rights are revoked when a Workforce member leaves the organization.
- Documenting a procedure to ensure that Workforce members remove any University ePHI from any personally owned device.

The procedures must comply with the Identity and Access Management policy and adhere to the following additional time constraints related to sections D (Deprovisioning) and E (Auditing) of that policy:

- Terminate access to ePHI immediately when such access is no longer required.
- Retain audit records for 1 year.
- Complete quarterly Account and Authorization Audits.

8.2.4 Technical Controls

Technical controls employ software and logical controls to prevent unauthorized activity that may pose a threat to the confidentiality, integrity or availability of ePHI.

Technical controls are often complex and may require controls beyond those specified in this Policy. The HIPAA Contact is responsible for ensuring the application of required technical controls, though the work of implementation is most likely performed by an IT Support Unit. The HIPAA Security Officer and Information Security are available to assist BU Health Plans with technical control selection and implementation advice.

8.2.4.1 Authentication

All access to ePHI must require authentication, ideally two-factor authentication when possible. University computer systems should rely on the University's central authentication system (Kerberos, Duo) and comply with the Data Protection Standards for Identity and Access Management. As is the case with our central authentication system, each individual accessing a system or application must be identified uniquely and account credentials may not be shared. Where shared accounts are required their existence and purpose must be documented.

Password Policy
Accounts with access to ePHI must require strong passwords as specified in the University's Data Protection Standards for Identity and Access Management.

Idle Timeout / Automatic Logoff
Systems and applications must require authentication when left idle for a few minutes, but no longer than 15 minutes. See Minimum Security Standards.

8.2.4.2 Authorizations

Ensure that individuals have only the authorizations required to perform their job function and no more. Be as granular as possible within the system or application. For example, if a Workforce member does not need the ability to write into a record and a read-only authorization is available, prefer the read-only role.

Accounts with Administrative Rights
Only grant administrative rights to systems and applications where required for job function. Ensure that individuals with higher privileges to manage or administer applications and systems understand what privileges they have and the need to use them responsibly.

8.2.4.3 Encryption

Encryption is the most basic protection that is so easy to provide with modern systems that its use should be ubiquitous. There are two types of encryption that must be considered: *Encryption in Transit*, where the ePHI is traveling across the network or through the electronic components of a system and *Encryption at Rest*, where the ePHI is stored in a tangible medium. In both types of encryption the goal is to protect the Confidentiality and Integrity of the data.

Encryption at Rest: All Devices
All devices (e.g., desktop computers, laptops, phones, USB thumb drives, CDs, backup tapes) used to access or store ePHI must use *Encryption at Rest* to protect the data if the device is lost or stolen. Any devices, either personal or University owned, that access or store ePHI and do not use encryption at rest must be documented, including why it was not reasonable and appropriate to implement encryption, and identification of an equivalent alternative security measure. The decision must be approved by the HIPAA Security Officer.

Encryption at Rest: Data Centers
Whenever possible, ePHI within data centers should be encrypted. The University recognizes that in some cases encryption on servers can present challenges particularly for service

availability. For example, the entry of a password to decrypt a system disk on a server may result in a significant outage if the system administrator is not available to provide it when an unanticipated reboot occurs. For systems that reside within a physically secure data center, the physical security may be an adequate compensating control for *Encryption at Rest*. The decision to not use encryption at rest must be documented, including why it was not reasonable and appropriate to implement encryption, and identification of an equivalent alternative security measure. The decision must be approved by the HIPAA Security Officer.

Encryption and Integrity Controls in Transit

All ePHI must be encrypted in transit and must use integrity controls. While there are a few methods of doing this, almost all of it uses Secure Socket Layer (SSL) or IP Security (IPSec) technology. In some cases it may be necessary to transmit unencrypted ePHI over an internal private network, such as that which resides within a data center rack, to provide compatibility with required legacy services that cannot support encryption or to enable real-time compute-intensive processing of data. The decision to not use encryption and integrity controls for ePHI transmission must be approved by the HIPAA Security Officer and documented, including why it was not reasonable and appropriate to implement, and identification of an equivalent alternative security measure.

Encryption Key Management

Encryption keys must be managed well. Guidance for implementing this control is specific to the technology and environment. IT Support Units setting up encryption should consult with the HIPAA Security Officer and Information Security for guidance.

8.2.4.4 Malicious Software Protection (Antivirus)

All systems must run a supported software package approved by the HIPAA Security Officer for detecting and preventing the execution of malicious software. The most common example is antivirus software, but other product types are emerging. An approved form of malicious software protection must be installed on all platforms that access ePHI, must run at all times, and must be set to automatically update and scan. Detections of malicious events as well as software in need of update must be reported centrally and monitored by the BU Health Plans' IT support.

8.2.4.5 Backups

BU Health Plans have an obligation to ensure all ePHI is constantly available, even in the aftermath of an unplanned event or disaster. BU Health Plans must have a procedure that is aligned with the System and Application Inventory. The procedure should:

- Cover both the loss of a physical drive, server, or facility (total loss of data), and loss of a specific file (e.g., through accidental deletion or corruption of the contents).
- Rely on the use of supported software. If the BU Health Plans rely on an external party to provide the backup solution, the BU Health Plans should ensure that the solution provider can meet the Component's needs for restoration of data during an emergency.
- Specify a frequency of backups that is acceptable to the BU Health Plans management and covers both partial and total loss of data (e.g., daily).
    - Ensure a backup is taken before any work is performed on a system, including but not limited to physically relocating a system or device within a facility.
- Ensure that all ePHI is backed up securely including backup to an alternate physical location.
- Ensure the backup media is inventoried and physically protected from theft.
- Retain backups for a period that is acceptable to the BU Health Plans from both a restoration of lost data and a limitation of storing too much data. Typical values range from a few months to a year.
- Ensure backup media is encrypted, particularly if it uses removable media that is prone to going missing, such as tapes or CDs.
- Document recovery procedures that can be executed by any IT professional
- Require testing of restoration to ensure that a restoration in an emergency will succeed (and revise if not).

8.2.4.6 Enable System and Application Auditing

The proper configuration of auditing must be applied for each application and operating system type. The following standards must be applied:

- Systems and applications with access to ePHI must log all authentication events: both log on and log off, both success and failure.
- Systems and applications with access to ePHI should log all access to ePHI, including read-only access where possible, and log all changes to the ePHI.
- Logs must be stored on the local system for at least 7 days but no more than year.

- Logs must be forwarded or automatically copied to a central log repository and retained for a year. Information Services and Technology has a Central Log Repository that is available for BU Health Plans to use if desired.

Additional recommendations may be found in the Minimum Security Standards within the University's Data Protection Standards. Information Security may also be consulted on recommended settings for a particular application or system.

8.2.5 Physical Controls

Physical controls are the most visible and common way we protect data. When implementing security for ePHI it is important to consider physical threats to the data as well as technology threats. One of the common ways data is lost is through physical access, tampering, and theft.

Physical controls include building elements like walls, doors, windows, counters, and locks as well as elements like video surveillance, alarm systems, and other theft deterrents such as lockable cabinets and drawers. It also addresses how physical space is used, such as not storing ePHI in predominantly public spaces or requiring visitors to pass through the record's room to access other parts of the facility.

BU Health Plans, with the guidance of the HIPAA Security Officer, will develop a facility security plan for every facility, and are encouraged to consult with Information Security, Space Management, Facilities Management and Planning, and Public Safety or the BU Police Department regarding their physical security concerns.

8.2.5.1 Ensure Facilities and Business Processes Protect ePHI

This HIPAA Contact, with support from management, is responsible for ensuring that reasonable precautions are taken to prevent physical access to ePHI during the course of normal, daily operations. This means that workstations used for accessing ePHI should not be accessible to the public, monitors displaying ePHI should be pointed away from public areas, servers must be kept in locked data centers with appropriate environmental controls, and portable devices must not be stored in areas where they can be easily stolen. In addition, business processes should reflect the need to secure ePHI and should not introduce vulnerabilities to otherwise secure data.

8.2.5.2 Workstation Physical Security

Devices outside of a data center that store unencrypted ePHI and that are not intended to be mobile must be physically secured using locking pads, cables, or similar technologies, unless stored in a significantly secured physical space.

keys_infosec

Image not found or type unknown

Theft of computing devices contributes significantly to the loss of ePHI. If a device containing unencrypted ePHI is stolen it is reportable breach.

Computer systems in public spaces, high traffic areas, or anywhere screens may be viewed from a distance must use privacy films to make it more difficult for an unauthorized person to read the screen.

8.2.5.3 Workstation and Device Use Procedure

The BU Health Plans must have a written procedure concerning workstation use that includes:

- A reference to the Boston University Conditions of Use and Policy on Computing Ethics.
- A reference to the Individual Responsibilities.
- An overview of key security controls on the workstations including requirements to log on, log off, inactivity time outs, and antivirus software;
    - Workforce members may not disable or bypass these mechanisms.
- A statement requiring that only IT support staff are permitted to install software on University workstations and devices.

The HIPAA Contact will need to tailor the procedure to fit the BU Health Plans, including by addressing:

- Where ePHI must be stored,
- Whether Personally-Owned Devices are permitted,
- The approved method for remote access to ePHI, if any,
- Whether removable media for ePHI and media management may be used, and
- Who the Workforce should contact to obtain computing support.

Advice on these decisions is included in the following sections.

Storage of ePHI

The BU Health Plans' procedures will specify the systems, workstations, devices, and drives where ePHI may be stored.

Personally-Owned Devices

The BU Health Plans' procedures must address whether its Workforce members are permitted to use personally-owned devices to access and store ePHI. The BU Health Plans should consider this as a risk-based decision based on factors such as:

- The type of services provided by the BU Health Plans including:
- The mobility requirements of the Workforce while providing services;
- The need for access to data outside of normal business hours for purposes such as:
  - to facilitate emergency care;
  - to support a 24-hour call center;
- The quantity of the ePHI being accessed;
- The ability of the Workforce to appropriately secure personally-owned devices; and
- The capability of the BU Health Plans to track personally-owned assets, monitor their use, and validate that appropriate controls are in place.

Remote Access to Campus Services

The BU Health Plans' procedures must address whether its Workforce members are permitted to access any systems containing ePHI remotely. If permitted, this should be enabled through the use of Remote Desktop or Virtual Private Network (VPN).

Removable Media and Media Inventory

The BU Health Plans' procedures must address whether removable media such as CD-ROMs, DVDs and thumb drives may be used to store ePHI. If allowed, the procedure must require encryption of the ePHI, and the HIPAA Contact must create and maintain a Removable Media Inventory that labels, inventories, and tracks the location of each device. Reusable devices must be securely erased before reuse or disposal. See Section 8.2.5.7: Equipment Disposal.

A BU Health Plans must be able to produce records about where ePHI has been stored and where all the media is currently located. The removable media inventory is separate from the System and Application Inventory.

8.2.5.4 Data Center Access Controls

If a BU Health Plans will run its own data center, the facility must use strong physical controls approved by the HIPAA Security Officer, including door locks, multi-factor authentication, video surveillance, and alarm systems. The HIPAA Contact will create a procedure that describes how access to the data center and surrounding facility is managed. BU Health Plans, using only IS&T Data Centers, do not need to create any new documentation.

In creating a procedure, it is important to consider visitor and vendor access to the facility and how access to the facility may be granted or extended under emergency conditions, including the need to have multiple vendors working simultaneously to restore service. IS&T's data centers conform to our Secure Data Center Access Policy which may be used as a reference.

8.2.5.5 Badges

All Workforce members must have a method of being positively identified by other Workforce members. For most purposes this is the Boston University ID Card, but for specific functions or areas it may be desirable for BU Health Plans to use a different or more visible form of badging. In addition, vendors and guests in areas that provide access to ePHI must either be escorted or have visitor badges. Badging should be coordinated by the HIPAA Contact.

8.2.5.6 Maintenance Records

BU Health Plans are responsible for understanding all work that is being done within their facility that impacts security including changes to hardware, walls, doors, and locks. While this work is generally performed by the University as a service to the BU Health Plans, the HIPAA Contact must document all repairs and modifications to physical components that may impact the security of ePHI and take any extra precautions necessary to protect data during maintenance periods.

8.2.5.7 Equipment disposal

When physical media such as hard disks, CD-ROMs, DVDs, or USB storage devices ("thumb drives") has reached the end of its service life it must be destroyed in accordance with the University's Data Protection Requirements and Destruction of Paper Records and Non-Erasable Media. Specifically, hard disks that contained ePHI must be disposed of via Information Security's disk drive shredding program, even if the ePHI was encrypted. This service is available free of charge.

Failed hard drives containing unencrypted ePHI must not be returned to the equipment manufacturer. Most equipment manufacturers will provide a mechanism to purchase a replacement disk without returning the old disk.

The HIPAA Contact must maintain logs of the proper disposal of electronic media on the Removable Media Inventory.

8.3 Phase 3: Detect

The detection phase involves ongoing monitoring of security controls to guard against unauthorized access to PHI. The components in this phase are:

1. Network Security Services (Section 8.3.1)
2. Information Security Activity Review (Section 8.3.2)

8.3.1 Network Security Services

Information Security provides Network Intrusion and Vulnerability Detection services to BU Health Plans as defined in the Education, Compliance, and Remediation Policy in the Data Protection Standards. The Incident Response Team reviews these events and will notify the HIPAA Privacy Officer and HIPAA Security Officer of events of concern that may require further investigation.

8.3.2 Information Security Activity Review

The BU Health Plans must implement a procedure that validates the BU Health Plans' security controls and ensures that violations of this Policy or the BU Health Plans' related procedures are detected, contained, and addressed. The HIPAA Contact must ensure reviews are conducted periodically (e.g., monthly) and documented.

A security review will include a detailed review of system and application audit logs to identify security events such as:

- Unauthorized access to systems or applications that create, receive, maintain, or transmit ePHI.
- Abnormal access to these systems or applications, such as:
    - Access at unusual times for a Workforce member;
    - Access from unusual locations;
    - Access to an abnormally large number of records or records for patients other than those under the care of the Workforce member;
    - Unusual alteration of health records; or
    - Removal or attempts to remove health information.
- Unusual activity of systems, including unusual processes, connections, or connection attempts.
- Attempts to bypass security controls or alter system files.

keys_infosec

Image not found or type unknown

The Information Security Activity Review should inspect audit logs for events that the BU Health Plans are uniquely qualified to identify as abnormal, such as activity by a Workforce member who is on vacation.

In addition, the Information Security Activity Review should include reviewing the status of controls to ensure they are functioning properly and proper maintenance is being performed. For example:

- Are system and applications being appropriately patched to eliminate vulnerabilities?
- Are antivirus systems in place, updated, and running properly?
- Are encryption controls in place, including data at rest (device encryption) and in transit (SSL required, secure, and using a valid certificate)?
- Are Workforce members following best practices around password management?

  - Controls around strength of password are in place and functioning.
  - Workforce members are not sharing passwords or posting them.
- Are workstations with access to ePHI physically secure from access and/or tampering?

8.4 Phase 4: Respond

A security incident is defined by the Security Rule as an “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system” (45 C.F.R. § 164.304).

If unauthorized access to PHI or loss of PHI is suspected, it is important that the event be thoroughly and properly investigated. This section covers:

1. Duty to Report Security Incidents (Section 8.4.1)
2. Duty to Respond (Section 8.4.2)
3. Periodic Security Incident Review (Section 8.4.3)

8.4.1 Duty to Report Security Incidents

keys_infosec

Image not found or type unknown

Any Workforce Member who suspects a security incident may have occurred must immediately notify his or her supervisor and the BU Information Security Incident Response Team at irt@bu.edu or 617-358-1100.

8.4.2 Duty to Respond to Security Incidents

The BU Health Plans have a responsibility to:

Identify, respond to, and report suspected or known security incidents;
Mitigate, to the extent practicable, any known harmful effects; and
Assist with documenting security incidents and their outcomes.

The HIPAA Privacy Officer, HIPAA Security Officer, and Information Security will assist with known or suspected breaches of ePHI and help the BU Health Plans meet their responsibilities for mitigation and documentation.

For more information, see the HIPAA Privacy Policy at Section 7: Breaches.

8.4.3 Periodic Security Incident Review

The HIPAA Security Officer will review past security incidents with the assistance of HIPAA Contacts at least annually to ensure completeness, accuracy, and find opportunities for improvement of controls and procedures.

8.5 Phase 5: Recover

Successful recovery requires careful planning for the unexpected, including Contingency Planning (Section 8.5.1).

8.5.1 Contingency Planning

The BU Health Plans must document how they will protect ePHI during an unforeseen event in a contingency plan. An unforeseen event could include a malicious event such as a cybersecurity attack to gain access to ePHI or to deny service, a routine physical system failure such as hard disk failure or network outage, a power outage caused by a utility failure, or a natural disaster such as fire, flood, or earthquake. The Security Risk Assessment and System and Application Inventory will help the BU Health Plans to determine which risks are most likely to occur and thus prioritize planning.

keys_infosec

Image not found or type unknown

The HIPAA Contact is responsible for maintaining the BU Health Plans' contingency plan as it relates to protecting ePHI. It is critical that management of the BU Health Plans participate in review and approval of the contingency plan.

8.5.1.1 Emergency Management Plans

Emergency Management Plans are based on the needs of the BU Health Plans. These plans capture what actions are taken during an emergency by the Workforce.

While portions of Emergency Management plans, such as evacuation of a facility, may be provided by other University policies and procedures, there are portions of emergency response plans that must be designed by the BU Health Plans. The plans include:

- Workforce responsibilities in responding to an event.
- Emergency communication plans, including phone lists and rally points.
- How emergency management plans will be disseminated, trained against, tested, and revised for viability.

8.5.1.2 Emergency Mode Operation Plan

An emergency may be more than an evacuation; a portion of a facility may be impacted for a period of days, weeks, or months. During this period, the BU Health Plans operate in "Emergency Mode". An Emergency Mode Operation Plan helps to ensure the confidentiality, integrity, and availability of ePHI. The HIPAA Contact is responsible for maintaining the Emergency Mode Operation plan.

keys_infosec

Image not found or type unknown

Emergency Mode Operations may involve operating at a diminished capacity or from an alternate location, potentially for an extended period of time. Some IT services on which the component depends may not be immediately available.

The Security Risk Assessment and System and Application Inventory will help the BU Health Plans understand what risks are likely to surface and what the impact will be. The BU Health Plans should plan for those risks, including the following topics:

- In the event of a prolonged emergency, will the BU Health Plans continue to operate?
    - Who has the authority to make such a decision?
- How will access to facilities be controlled during an emergency?
- What technology components are required to provide enrollment and claims services?
- How will missing technology components be compensated for in terms of:
    - ePHI that may be temporarily unavailable to the BU Health Plans;
    - ePHI generated by the BU Health Plans (if any) that cannot be stored in the normal manner.

External Dependencies

In developing the Emergency Mode Operations Plan, the BU Health Plans should also consider their external dependencies for providing service. The BU Health Plans may be dependent on the provision of Internet services to connect to cloud services or on enterprise authentication services to log in to desktops and workstations. Emergency planning should encompass what to do if services outside of the BU Health Plans' control are unavailable even if the Component itself is not directly affected.

Restoration of Normal Service

When planning for a disaster it is important to also consider how normal service would be restored. Consider, for example:

- The technology resources required to resume normal service;
- How PHI generated outside of the electronic system during the emergency will be entered into the electronic later; and
- Who will be responsible for the data entry.

The details of the Emergency Mode Operation Plan will likely highlight a few more considerations for the restoration of service plan.

8.6 Ongoing Maintenance of Security

The five phases of the Cybersecurity Framework are meant to be iterative. Completion of the five phases should be followed by starting again at the beginning.

keys_infosec

Image not found or type unknown

Security is a journey not a decision.

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