Effective Date: **August 1, 2013** Revised: **October 29, 2021**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY, RESEARCH AND SCHOLARLY ACTIVITIES

HIPAA Policies for Healthcare Providers at Covered Components: Policy 8, HIPAA Security Program

RESPONSIBLE OFFICE

Research Compliance

This Policy 8 is part of the HIPAA Policy Manual: Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components.

Philosophy

Boston University's HIPAA security program integrates the HIPAA Security Rule requirements into the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF identifies the key, ongoing steps as: Identify, Protect, Detect, Respond, and Recover. This section is organized according to these five phases:

Image not found or type unknown

Security Program Structure: Phase 1 - Identify, Phase 2 - Protect, Phase 3 - Detect, Phase 4 - Respon

Responsibility for the security of patient information is shared between the HIPAA Components, BU IS&T and other BU central services. The sections below delineate the responsibility of each in specific areas. The BU HIPAA Privacy and Security Officers support the HIPAA Contacts in carrying out their responsibilities.

These polices are supplemented by Covered Component procedures based on the unique risks and needs of the individual Covered Components.

BU has other University-wide policies that impact information security, including but not limited to the Information Security Policy and the Data Protection Standards. These are not repeated in this Manual, but certain policies are referenced and linked in this document.

Defined Terms

Device: any electronic item that stores and processes (does something to or with) electronic data. This broad term includes desktop computers, laptops, tablets, mobile phones, medical devices, printers and fax machines that contain hard drives, and anything else that can store and process electronic data. Devices may be owned by BU or may be personal devices owned by the workforce member.

Media: any item that can store but not process data, including USB drives, CD-ROMs, DVDs, hard drives, back up disks.

Application is a computer program that processes information. Examples are Microsoft Outlook; electronic medical record programs; and programs that allow the sending and receiving of electronic data.

System means one or more computer servers and their related applications. For example, an electronic record system is composed of the servers, the electronic medical record application, the backup function and related applications.

Data Center is a physical location where servers are kept.

8.1 Identify

PHI can be protected only when we understand what it is, where it is, and who is authorized to access and use it. To that end, each Covered Component is responsible for identifying their PHI, where it is allowed to be stored, the members of their workforces, roles of their workforce members, and a process for providing, modifying and removing individual access to PHI.

8.1.1 PHI Inventory

BU IS&T (and GSDM IT for the Dental Health Centers) inventory and track all **BU** *devices* (except for iPads, phones, medical devices, and fax machines) through its KACE system, and ensures those devices meet BU device standards for devices that access BU Restricted Use Data.

Covered Components document in their procedures:

- where PHI may be stored;
- whether its Workforce members are permitted to use personally-owned devices to access and store PHI;
- whether and how its Workforce members are permitted to access any systems containing PHI remotely;
- whether removable media such as CD-ROMs, DVDs and thumb drives may be used to store PHI and if so, how such media will be inventoried and tracked and what security measures must be followed.

The Covered Component PHI Inventory lists all BU iPads, BU phones, BU medical devices, and fax machines permitted to store PHI. The inventories are maintained on the BU HIPAA SharePoint. HIPAA Contacts must ensure the Inventory is kept up to date and conduct periodic reviews to confirm. The inventory includes:

- Identification information, such as name, description, classification, identifier or IP
- Owners or administrators, such as Microsoft Team site owners who can add/remove team members or people who can add/remove people from third-party websites/apps
- Normal location, such as floor/room
- Backup mechanism or procedure, such as “None,” “Locally Managed,” “IS&T Managed,” or “Vendor Managed”
- Restoration priority (1-5, with 1 being the highest priority) for IT Support to know what to restore first. For example, restoration of a medical record system might be priority 1,

while SharePoint might be priority 2 and a transcription service might be priority 3 or 4. Components should note that services may not get restored in exactly this order, depending on many things including the nature of the issue(s), availability of resources, and shared value with other units. However, in the scope of an outage that impacts only the Covered Component, it will be of great value to have alignment with component management on where IT Support should try to focus first.

Workforce members, permitted by Covered Component procedures to use personal devices, must implement Restricted Use Minimum Security Standards safeguards and document compliance as part of annual HIPAA training, and before a new device is used. For example, a workforce member at a Sargent College HIPAA Component will complete an attestation as part of annual HIPAA training – generally September of ever year – and complete it again when they get a new phone or laptop. HIPAA Components at BU Charles River Campus document compliance on Blackboard. Workforce members at Dental Health Centers document compliance on the Dental Portal.

8.1.2 Security Risk Assessments

The HIPAA Security Officer, working with the HIPAA Contacts, Information Security, and Internal Audit & Advisory Services and, from time to time as needed, external consultants, is responsible for conducting a comprehensive Security Risk Assessment that meets the requirements of the HIPAA Security Rule. The assessment will, *inter alia*, document and prioritize all reasonably anticipated, high-level administrative, physical, and technical risks to the confidentiality, integrity, and availability of PHI.

The Security Risk Assessment confirms where PHI is located and identifies threats, vulnerabilities, risks, and controls, including an assessment of:

- threats to and vulnerabilities of those systems
- existing controls and countermeasures that mitigate those threats and vulnerabilities
- likelihood the vulnerabilities will be exploited by a threat
- potential impact of such threats and vulnerabilities on the confidentiality, integrity, and availability of PHI

These four factors (i.e., threats, vulnerabilities, likelihoods, and impacts to PHI) are combined 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 create a Corrective Action Plan to address each identified risk. A summary of such assessments shall be made available to the Common Services and Information Security Governance Committee and others, as deemed appropriate.

The HIPAA Security Officer will perform or oversee a comprehensive risk assessment at least every 3 to 5 years. In the interim, the HIPAA Security Officer and Covered Component HIPAA Contacts shall review it at least annually and update it as needed on an ongoing basis, as described in the next section.

8.1.3 Periodic Technical and Non-Technical Security Reviews

The HIPAA Security Officer shall conduct periodic technical and non-technical reviews of the security of PHI to assess whether existing physical, technical, and administrative controls meet the requirements of this Policy and the Covered Components' procedures. Reviews may involve inspecting system configurations, conducting vulnerability scanning or penetration testing, auditing documentation, checking physical controls such as doors and locks, looking at how devices are physically secured, verifying alarm and video systems are functioning, and other controls. These reviews may include an examination of security practices of Business Associates.

Security review findings shall be documented in the BU HIPAA SharePoint site and may require a Covered Component response. When security reviews identify correction actions for Covered Components, the HIPAA Contacts are responsible for ensuring timely completion of the corrective action. Likewise, the HIPAA Security Officer, IS&T, or Dental IT are responsible or ensuring timely completion for corrective actions assigned to them.

The HIPAA Security Officer should periodically review risk analyses of technology, and where appropriate conduct a full or partial review to assess any new risks.

HIPAA Contacts are required to ask the HIPAA Security Officer to conduct a security review before purchasing new technology or implementing any changes affecting the administrative, technical, or physical controls that protect PHI.

HIPAA Contacts must notify the HIPAA Security Officer of any changes in the environment, operational procedure, or significant changes in the risks to PHI so that the Security Officer may perform an updated review. Often these involve new systems, applications or other changes that may affect the security of PHI. These reviews may have a smaller scope, such as the planned acquisition of a new software package or physical relocation.

8.2 Protect

8.2.1 Individual Responsibilities

See Section 2 of this HIPAA Policy Manual.

8.2.2 Administrative Controls: Training, Access Management

Training: See Section 1.8: HIPAA Training.

Security training is part of annual HIPAA training. In addition, the HIPAA Security Officer will periodically issue reminders and updates about security issues of critical concern. Covered Components will ensure these reminders reach all members of the Covered Component Workforce.

Access Management: Covered Components create and document procedures that build upon the procedures below to define how access to PHI is authorized, maintained, and revoked, including a matrix of access rights based on Workforce member roles, following the Minimum Necessary standard (see Policy 3.2).

The Dental Health Centers maintain their documentation of changes to access rights (provision, modification, or revocation) on the GSDM "portal." The other Covered Components maintain this documentation on the BU HIPAA SharePoint site.

Access to PHI is provided only after HIPAA training is completed, is modified when a workforce member's role changes, and is revoked immediately (e.g. within 24 hours) when such access is no longer required due to a workforce member leaving a role, unless an Exception is granted pursuant to Section 10.0.

Provision

When a new staff member is hired at a Charles River Campus HIPAA Component, the HIPAA Contact enters a new Access Request on the Covered Component HIPAA SharePoint site. In the request, the HIPAA Contact confirms the workforce member has completed HIPAA training. HIPAA Contacts are Blackboard Instructors for the HIPAA Training, giving them the ability to add users and verify staff have completed training and a security attestation for any personal devices.

IS&T receives a HIPAA SharePoint site alert when a new access request is made by a HIPAA Contact or Covered Component management. IS&T enters a date for the “IT Fulfilled” column of the Access Request list when they have made the technical change according to the request and the Covered Component access matrix maintained on the HIPAA SharePoint site.

Modification

Modifications occur less frequently but need to be documented on the HIPAA SharePoint site for any role changes, such as a different type of medical or dental record account.

Revocation

Revocation should include an interview or exit training, prior to the last day of employment. The interview or training should remind the workforce member of their ethical duty to keep patient data private (no sharing) and secure (destroyed or returned to BU). Any PHI held outside Covered Component systems must be returned or destroyed as appropriate.

At the conclusion of employment, unless infeasible, the HIPAA Contact or management asks the workforce member to sign an exit attestation (paper or electronic) or confirm by email that they have returned or destroyed all patient and research subject data.

Example:

> “I (first last) confirm that I have securely destroyed or returned all patient and research subject data to the Danielsen Institute. This includes data in email systems not approved for Restricted Use or on personal devices, in download folders or trash folders.”

When physical access to HIPAA Component facilities is no longer required, the HIPAA Contact or management takes all steps necessary to remove physical access, including retrieving any physical keys, making a request for any badge access to be removed, and changing any shared entry codes or passwords. Changes are tracked in a Physical Security

Log maintained on the Covered Component HIPAA SharePoint site.

When technical access is no longer required, the HIPAA Contact submits an Access Request for revoking access. The HIPAA Contact removes or disables any HIPAA Contact managed access, such as an electronic medical record, and requests that IS&T remove IS&T managed access, such as network drives. After removing access, IS&T enters a date in the “IT Fulfilled” column of the Access Request list.

Access Review

Ideally quarterly, but at a minimum annually, the HIPAA Contact reviews the records for Access Management to confirm all staff have minimum necessary access to PHI. For example, have all staff been assigned to the right access role? Have all former staff electronic medical record accounts been disabled or removed?

The Access Review should be documented. Charles River Campus HIPAA Components can enter a new date in the “Reviewed” column of the HIPAA SharePoint site Access Request list.

8.2.3 Technical Controls

Technical controls are software and logical controls to prevent unauthorized activity that may pose a threat to the confidentiality, integrity or availability of PHI. Following are technical controls common to all:

- Accounts with access to PHI require strong passwords as specified in the University’s Data Protection Standards for Identity and Access Management.
- Access to PHI requires two-factor authentication wherever possible. When two-factor authentication is not possible, quarterly password changes is an acceptable alternative.
- Each individual accessing a system or application is identified uniquely and account credentials may not be shared, unless approved by an Exception pursuant to Policy 10.
- Shared email accounts used for patient or research subject communication, or otherwise containing HIPAA data, must have a forced quarterly password change and be audited on an annual basis as part of the Information System Activity Review procedure.
- When applications have the capability (such as BU REDCap), accounts should be set to automatically disable after six months of inactivity, requiring administrator approval to make the account active.

- Systems and applications require authentication when left idle. Maximum idle time for PHI systems or applications is 15 minutes. Alternatively, the device idle time may be set to 15 minutes, without signing out of a particular application.
- Administrative rights to systems and applications are granted only where required for job function.
- Removable media have been blocked from all BU devices in the Covered Components using Microsoft Group Policy, except for those devices or removable media that the Security Officer and HIPAA Contact agree are necessary. HIPAA Contacts are responsible for including every permitted device and removable media in the Covered Component Inventory
- Servers and devices must comply with the BU Data Protection Standards, Minimum Security Standards. In addition, servers and devices require the following:
    - Production system changes must follow the BU Change Management Procedure
    - Production environments must meet Covered Components availability needs (e.g., load balance, failover)
    - Test environments must contain de-identified HIPAA data or meet the same control requirements as the production environment
    - All maintenance provided by vendors or personnel not part of IT Support must be actively monitored (i.e., watched) by IT Support, either physically or using technology such as BU Teams
    - Servers must have a private IP that is not accessible from off-campus
    - Server firewall rules must limit access to the minimum necessary ports and protocols required for the system to operate
    - Server firewall rules must limit on-campus connections to the IP range of the school or department, unless the service (e.g., BU Restricted Use network drive) is accessed from all over the BU campus
    - Server firewall rules can permit off campus access through a BU VPN or a network address translation service (e.g., load balancer or Campus Edge NAT service)
    - Server firewall rules must be audited periodically by BU Information Security in coordination with HIPAA Contacts and IT Support
    - Servers must be scanned by BU vulnerability scanner and included in the BU Information System Activity Review Procedure, Knowledge Base Article (KBA) in BU ServiceNow
    - Servers must be also be in data centers protected with IDS or IPS as deemed appropriate by BU HIPAA Security Officer

- Covered Components facilities must have private BU networks that are isolated from non-Covered Component subnets
- Covered Components must use BU networks (i.e., wired network, wireless network, or VPN when off-campus), never using personal Wi-Fi hot spots or non-BU networking gear, unless connecting from off-campus and using a BU VPN

Additional technical controls specific to each Covered Component are documented in their HIPAA procedures.

8.2.3.1 Encryption

Data Centers: PHI within data centers is encrypted at-rest, except where the HIPAA Privacy and Security Officers have granted an exception pursuant to Policy 10 of the HIPAA Policy Manual.

Devices: All devices (e.g., desktop computers, laptops, phones, USB thumb drives, CDs, backup tapes) used to access or store PHI 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 PHI and do not use encryption at rest must be documented as an Exception pursuant to HIPAA Policy 10.

Transmission: All PHI must be encrypted in transit and must use integrity controls except where the HIPAA Privacy and Security Officers have granted an exception pursuant to Policy 10 of the HIPAA Policy Manual.

8.2.3.2 Anti-malware Software Protection

All systems that store or access PHI must run anti-malware software approved by the HIPAA Security Officer for detecting and preventing the execution of malicious software.

BU IS&T will install anti-malware on all BU systems, devices and applications that access PHI. Covered Components are responsible for ensuring permitted personal devices have anti-malware. BU IS&T offers anti-malware at no cost for both BU and personal devices.

Anti-malware must run at all times and must be set to automatically update and scan.

8.2.3.3 Backups

All systems and applications that store PHI must be securely backed up. Covered Components describe the backup mechanism or procedure for each in the Covered Component Inventory. Backups must be periodically tested by IS&T and GSDM IT in coordination with HIPAA Contacts. Security reviews of vendor provided services must include questions on backup processes and periodic testing.

8.2.3.4 System and Application Auditing

BU IS&T is responsible for auditing systems and applications run by BU IS&T centrally, such as RU-GPNAS network drives. Servers must forward logs to BU central log repository. Devices must have log storage (e.g., Windows Event Logs) increased to ensure at least three months of audit logs are stored on each device. Device logs are not forwarded but are necessary for Incident Response Team investigations. Covered Components document auditing procedures for applications unique to each, such as Component electronic medical records.

8.2.4 Physical Controls

8.2.4.1 Covered Component Facility Physical Security Plan

Each Covered Component has a floor plan maintained by Boston University Real Estate and Facility Services that documents the physical structures, such as rooms and locking doors that protect PHI from theft and other physical threats. The Security Officer reviews these floor plans with each Covered Component and works with Boston University Real Estate and Facility Services to correctly document the physical structures. Plans approved by the Security Officer are stored on the HIPAA SharePoint site.

The Dental Health Centers maintain an inventory of keys (presently in CAMMS, BU Facilities Service Request system), where each key must be linked to a UID. Each department is responsible for deciding and tracking who gets keys, and reporting when any individual or shared key is lost. The other Covered Components maintain an inventory of physical keys on the BU HIPAA SharePoint site.

BUPD on the Charles River Campus and BU Public Safety on the Medical Campus provide security monitoring and response.

Boston University ID Card provides a method for positively identifying members of a Covered Component Workforce (UID). Vendors and guests in areas that provide access to PHI must either be escorted or have visitor badges.

The HIPAA Contact is responsible for ensuring that repairs and modifications to their physical components are managed in such a way as to maintain the security of PHI, are correctly documented in the Covered Component floor plan, and for contacting the HIPAA Security Officer for assistance as needed.

8.2.4.2 Data Center Physical Security

BU IS&T is responsible for the security of all BU IS&T data centers, including access control.

Any Covered Component that wishes to establish a new data center must consult the Security Officer and comply with the IS&T Data Center Policy.

8.2.4.3 Security in Business Processes

This HIPAA Contact is responsible for ensuring that reasonable precautions are taken to prevent unauthorized access to PHI during the course of normal, daily operations consistent with the BU Individual Responsibilities policy at Section 4.0 of this HIPAA Policy Manual. For example, devices used for accessing PHI should not be accessible to the public, monitors displaying PHI should be pointed away from public areas, servers must be kept in data centers that comply with section 8.2.4.2, and portable devices must not be stored in areas where they can be easily stolen. In addition, business processes must be designed to ensure data is kept secure.

8.2.4.4 Device and Media Security

HIPAA Contacts must list all devices not inventoried by IS&T or GSDM IT using KACE on the HIPAA SharePoint site Inventory. Devices must be encrypted, and generally not shared with other workforce members unless used for patient care (e..g, dental scanner).

Devices must be securely wiped before they are reused by another workforce member or used for another purpose.

Devices outside of a data center that have a documented Exception to store unencrypted PHI, 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.

Permitted personal devices must meet the same security standards as BU owned devices, which means the device:

- has been checked by IS&T or GSDM IT to confirm it has:
    - encryption turned on,
    - has anti-malware installed,
    - has an idle time of 15 minutes or less, and
    - has an operating system that is supported and regularly updated.

Workforce members must complete a security attestation annually and whenever a workforce member acquires a new device that will be used for accessing, processing, or storing PHI.

BU IS&T provides secure destruction of physical devices and media pursuant to the University's Data Protection Requirements and Media Destruction One-Sheets. This service is available free of charge.

Any device or media containing PHI that has reached the end of its useful life must be delivered to IS&T for secure destruction *even if* the PHI was encrypted.

IS&T and GSDM IT record destruction of KACE-controlled devices; Covered Components record destruction of other devices and media on their Inventories.

8.3 Detect: Information System Activity Reviews

BU IS&T monitors central systems such as the Campus Edge Firewall and notifies the HIPAA

Privacy Officer and/or HIPAA Security Officer of events of any concern that may involve PHI for their further investigation. IS&T continuously tests and improves their detective processes.

BU IS&T is also responsible for Information System Activity Reviews of BU-managed systems, devices and applications, including confirming appropriate patching and anti-malware systems are in place, updated, and running properly. GSDM IT performs this review for the Dental Health Centers' separate systems, devices and applications.

IS&T and GSDM IT reviews are documented in ServiceNow (BU's IT service tracking system) in accordance with a Knowledge Base Article that is maintained by the HIPAA Security Officer. IS&T and GSDM IT continuously test and improve detective processes.

The Covered Components are responsible for System Activity Reviews of any systems, devices and applications unique to them, for example, their electronic medical records or any medical devices. The plan for such review will be created jointly by the HIPAA Contact and HIPAA Security Officer, based on an assessment of the risks posed by the operations and nature of activities of the Covered Component, aimed at detecting e.g., unauthorized access, unusual uses, or suspicious disclosures. HIPAA Contacts are responsible for documenting the review plans in Covered Component HIPAA Procedures, and for documenting monthly reviews using the HIPAA SharePoint site "Monthly Activity Review" list.

8.4 Respond

A security incident is 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). Typically, only successful unauthorized access, use, disclosure, modification or destruction will constitute a breach under HIPAA, as determined by the HIPAA Privacy and Security Officers.

Any Workforce Member who suspects a security incident may have occurred must immediately notify his or her HIPAA Contact and the BU Information Security Incident Response Team at irt@bu.edu or 617-358-1100. Incidents may also be reported to hipaa@bu.edu or anonymously to the BU EthicsPoint. For more information, see Section 7: Breaches.

8.5 Recover: Contingency Planning; Emergency Mode Operations; Recovery

BU Emergency Management coordinates a comprehensive emergency management program designed to prevent, prepare for, respond to, and recover from any threat, emergency, or disaster that could disrupt HIPAA Component operations. To prepare for emergencies, HIPAA Contacts are responsible for creating and annually reviewing a Continuity of Operations Plan (COOP) with guidance from BU Emergency Management.

HIPAA Contacts must provide a COOP to BU Emergency Management and store a copy on their HIPAA SharePoint site. When COOPs are updated, the HIPAA Contact must likewise provide the updated COOP to Emergency Management and upload a copy to the HIPAA Component SharePoint site.

HIPAA Contacts are responsible for periodically testing their COOP, and conducting after action reviews of recovery plans to identify areas of improvement.

BU IS&T is responsible for responding to electronic emergencies, such as a cybersecurity attack to gain access to PHI or to deny service, or a network outage.

The healthcare services provided by BU's Covered Components are all outpatient services of an elective nature and therefore there is no plan to continue to provide services during an emergency. In all emergencies and disasters, the Covered Component Workforce will coordinate with BU Emergency Management Department and BU Police or Public Safety, to protect the safety of Workforce members and patients and physical assets, including those holding PHI.

Planned responses to specific emergency situations are described below.

- Unavailability of EMR: In the event the Covered Component's EMR is unavailable for more than a brief time, providers will record information physically using pen and paper, or electronically using available electronic resources (such as Microsoft Word). Any physical records created will be secured in accordance with the standards provided in Section 2.0 of the HIPAA Policy Manual. Any electronic PHI created outside the medical record must be stored in a location approved for PHI and Restricted Use Data, such as Microsoft OneDrive or an approved network drive. Upon the reactivation of the EMR, the HIPAA Contact and clinical leaders of each affected component will meet to determine how the physical PHI will be added to the EMR to ensure the completeness and integrity (for example, following a brief interruption, providers may be responsible for entering all data themselves and destroying securely all physical PHI that has been electronically entered). If the duration of the interruption is long enough that this will be inefficient, the HIPAA Contact and clinical leaders will determine whether other members of the Covered Component workforce will assist; whether assistance will be provided by BU resources outside of the Covered Component, or whether external resources will be used. The usual rules apply. BU resources outside the Covered Component will be treated as Support Units and subject to the same obligations as Support Units. External resources will be required to execute a Business Associate Agreement before accessing PHI.

- Unplanned Destruction of Electronic Medical Records: Covered Components other than the Dental Health Centers use a third-party provider electronic medical record. Each of those third parties is responsible for backing up the data in the electronic medical record and will be key participants in restoring access and confirming the integrity of the data. The HIPAA Contact is responsible for coordinating this effort. GSDM IT is responsible for back up and restoration of Salud and Eaglesoft.
- Unplanned Destruction of BU Drives, Systems: IS&T is responsible for back up and restoration of any BU central systems and applications.
- Severe and Disabling Emergency: In the event of a severe emergency that renders a Covered Component incapable of providing any health services to its patients, patients will be directed to the nearest emergency facility for urgent medical needs. This will be done through a sign posted at the patient entrance of each such facility, by recorded message at the main telephone number used by patients, and online, as coordinated with BU Emergency Management Department. The HIPAA Contact is responsible for ensuring this is done. Following that step, the HIPAA Contact and clinical leadership of the component will meet to determine other appropriate steps that may include individual providers using reasonable efforts to contact patients deemed to be in immediate need of care to assist them in making alternate care arrangements.
- When Physical Space is Unavailable: Physical space regularly used by Covered Components to provide health services may be rendered unusable for an extended

period of time by fire, flood, earthquake, terrorist attack and other natural and man-made disasters. If this occurs, BU Emergency Management Department and Facilities Management will head the effort to secure an alternate location. The HIPAA Contact, with the support of the BU HIPAA Privacy and Security Officers, will ensure such alternate locations meet BU's HIPAA standards and/or for approving temporary Exceptions pursuant to Section 10.0 of this HIPAA Policy Manual.

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