PAISBOA
HEALTH BENEFIT TRUST

THE TRUSTEES OF THE PHILADELPHIA AREA INDEPENDENT SCHOOL BUSINESS OFFICERS ASSOCIATION HEALTH BENEFIT TRUST

THE PHILADELPHIA AREA INDEPENDENT SCHOOL BUSINESS OFFICERS ASSOCIATION HEALTH BENEFIT PLAN

# HIPAA Security Policies and Procedures

**Effective July 1, 2023**

## TABLE OF CONTENTS

**Page**

## SECURITY POLICY STATEMENT

These Security Policies and Procedures are designed and intended to ensure[1] the Philadelphia Area Independent School Business Officers Association Health Benefit Plan (the "Plan") complies with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Standards (the "Security Standards").[2] The Plan is sponsored by the Trustees of the Philadelphia Area Independent School Business Officers Association Health Benefit Trust ("Plan Sponsor").[3]

The Plan Sponsor is the Plan Administrator, responsible for administering the Plan. The Plan Administrator has delegated day-to-day Plan administration authority to certain employees of the Plan Sponsor, referred to as "Privacy Employees" and to certain third parties referred to "Business Associates."

The Plan Administrator, the Privacy Employees and the Business Associates request, receive, use, store and disclose individually identifiable health information about participants and their dependents for the purpose of administering the Plan. This information is protected health information ("PHI") that is protected by the Security Standards and covered by these Security Policies and Procedures.

In addition, the Plan Sponsor, Business Associates, and their authorized agents may perform various non-administration functions related to the Plan, such as collecting enrollment information, deciding plan eligibility, remitting payment for premiums and claims advocacy. The information collected by the Plan Sponsor or its agents when it is performing these functions is not PHI and is not protected by the Security Standards or covered by these Security Policies and Procedures.

The Plan Sponsor, in its capacity as employer, may request, receive and store health information about its employees for employment-related purposes, such as preemployment testing, or to determine whether an employee is eligible for leave benefits under the Family and Medical Leave Act or an accommodation under the Americans with Disabilities Act. This health information, which is received and stored by the Plan Sponsor in its capacity as employer, is not PHI and is not protected by the Security Standards and covered by these Security Policies and Procedures.

The Plan adopts these Security Policies and Procedures to (1) ensure the confidentiality, integrity, and availability of all electronic protected health information ("ePHI") that it creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (4) ensure compliance with the Security Standards by its employees.[4]

---

1. The term "ensure" as used throughout these Policy and Procedures is not meant to guarantee compliance with the Security Standards. Rather, "ensure" shall mean the Security Officer, employees, Business Associates or others, as applicable, will use their best efforts to comply with the Security Standards.

2. This refers to the Privacy Rule, 45 C.F.R. Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health Act, which is at Section 13400, *et. seq.* of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 17921, *et. seq.*, and any regulations promulgated thereunder ("HITECH").

3. The Plan Sponsor sponsors benefits which are not covered by HIPAA and/or these Security Policies and Procedures.

4. The term "employees" refers to all individuals who work for the Plan Sponsor and fall within the definition of "workforce" under HIPAA. Specifically, "[w]orkforce means employees, volunteers, trainees, and other persons who conduct, in the performance of work for a covered entity, whether or not they are paid by the covered entity" 45 CFR 160.103 (definition of "workforce").

These Security Policies and Procedures will be amended and/or supplemented as necessary and appropriate to comply with changes in the law or regulations or other interpretation of the Plan's security-related obligations. The Security Officer will promptly document and implement any amendments or supplements to these Security Policies and Procedures.

In implementing and maintaining the security measures described herein, which reasonably and appropriately reflect the Security Standards, the Security Officer took the following factors into account: the size, complexity and capabilities of the Plan Sponsor and its Business Associates, the technical infrastructure of the Plan Sponsor and its Business Associates, hardware and software security capabilities of the Plan Sponsor and its Business Associates, the costs of the security measures and the probability and criticality of potential risks to ePHI.

## I. SECURITY MANAGEMENT PROCESS

**POLICY:** The Plan prevents, detects, contains and corrects security violations.

A. Risk Analysis (Required). The Plan has conducted an accurate and thorough initial assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the Plan. This assessment was reviewed by the Security Officer.

B. Risk Management (Required). The Plan has implemented the security measures described in these Security Policies and Procedures, which reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Standards.

C. Sanction Policy (Required). The Security Officer (designated in Policy II) in conjunction with the Privacy Officer will apply appropriate sanctions against employees who fail to comply with these Security Policies and Procedures.

1. Discipline**.** The Plan Sponsor has a zero-tolerance policy regarding the improper use, storage, maintenance or transmission of ePHI by any employee. Any Plan Sponsor employee who violates the Security Standards and/or these Security Policies and Procedures may be subject to sanctions, including, but not limited to, oral counseling, write-ups, suspension, and/or termination.

2. Discretion of the Security Officer**.** The Plan Sponsor does not guarantee that one form of discipline will necessarily precede another. Further, the Security Officer reserves the right, at all times, to take whatever disciplinary action the Security Officer deems appropriate, up to and including termination. Prior notification and progressive discipline are not prerequisites for termination or other disciplinary action. The Security Officer will impose disciplinary sanctions for any violation of these Security Policies and Procedures that the Security Officer deems appropriate.

D. Information System Activity Review (Required). The Plan has implemented the following procedures to regularly review records of information system activity.

1. Records of Information System Activity. The Plan generally does not maintain ePHI on the Plan Sponsor's systems. To the extent ePHI is received by Privacy Employees via encrypted email, it is deleted immediately. No enterprise-wide record of information system activity will be maintained.

2. Reviewer. The Security Officer will promptly review any and all reports of alleged violations of the Plan's HIPAA Security Policies and Procedures. The Security Officer will maintain a log that documents the final resolution of any reported incident.

## II. ASSIGNED SECURITY RESPONSIBILITY

**POLICY:** The Security Officer is responsible for the development and implementation of these Security Policies and Procedures.

A. **SECURITY OFFICER DESIGNATION.** The Security Officer is responsible for overseeing and directing the development and implementation of these Security Policies and Procedures in compliance with HIPAA's Security Standards.

1. Designated Security Officer. The Plan has designated the following Security Officer:

   Executive Director
   PAISBOA Health Benefit Trust
   301 Iven Avenue, Suite 315
   Wayne, Pennsylvania 19087
   (484) 580-8844
   executive.director@phbtrust.org

2. Duties and Responsibilities. The Security Officer is responsible, either directly or by delegated authority, for monitoring and ensuring the Plan's compliance with the HIPAA Security Standards and these Security Policies and Procedures. Specifically, the Security Officer has ultimate responsibility to ensure cybersecurity and information security across the Plan Sponsor and affiliates including as the following as it relates to ePHI:

   a. Oversees the development and implementation of HIPAA Security compliance processes, and controls the day-to-day aspects of compliance with the HIPAA Security Standards;

   b. Identifies HIPAA Security non-compliant processes and systems, and develops and implements those changes that are necessary to ensure all technical processes and systems that create, receive or maintain ePHI are HIPAA Security compliant;

   c. Serves as central liaison for Business Associates involved in HIPAA Security systems and processes, and for external business partners and vendors involved in HIPAA Security systems and processes;

   d. Communicates HIPAA Security compliance assessment findings, including cost and risk exposure, to the Plan and impacted employees;

   e. Tracks action items;

   f. Prepares budgets for HIPAA Security technical compliance;

   g. Oversees workforce training on HIPAA Security compliance;

   h. Reviews and revises these Security Policies and Procedures as required or needed to ensure continued compliance with the HIPAA Security Standard and any other applicable law;

i. Investigates any alleged security incidents, and/or any complaints that allege that the Plan, an employee or a Business Associate has not complied with or has violated these Security Policies and Procedures; and

j. Oversees all document maintenance and retention policies as required by the Security Standards.

## III. WORKFORCE SECURITY

**POLICY:** Through these authorization, clearance and termination procedures, the Plan ensures that the appropriate employees have appropriate access to ePHI, and that employees who should not have access to ePHI are prevented from obtaining such access.

A. Authorization and/or Supervision (Addressable). The Plan has implemented the following procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed. Only those employees with authorization may access ePHI.

1. Authorization.

a. Employees.

Employees who are authorized to access ePHI are those Privacy Employees which are described in greater detail under Policy III of the Plan's HIPAA Privacy Policies & Procedures. The Privacy Employees operate at privilege levels no higher than necessary to accomplish required job duties.

2. Locations. The locations where ePHI is created, maintained, accessed and/or stored are:

a. Physical Locations.

(i) Privacy Employees generally work from an office building in Wayne, Pennsylvania. The building has a receptionist.

(ii) From time-to-time Privacy Employees will work from their residences. No hard copy PHI is maintained at personal residences. Privacy Employees do not leave laptops unattended while in use and keep laptops in a locked drawer when not in use.

(iii) As specified in the Plan's Notice of Privacy Practices, the Plan generally does not maintain or store within its possession any PHI. PHI is routinely kept by the Plan's Business Associate that provides cloud-based benefit administration systems.

b. Technical Location.

(i) E-Mail. Privacy Employees do not generally email ePHI. If there is a need to email ePHI, such ePHI is password protected and/or encrypted.

(ii) Secure Websites. Privacy Employees may transmit, receive and review ePHI through secure, encrypted websites maintained by the Plan's Business Associates. These websites can only be accessed through passwords and the information entered into and transmitted through these websites is protected by the Business Associate's secure systems.

(iii) Laptop & Desktops. ePHI is not maintained on laptop or desktop hardware. If laptops or desktops are to be reused, they will be completely wiped and reimaged.

3. Supervision. Access to ePHI is supervised by the Security Officer as notified by Privacy Employees.

   a. The Privacy Officer, guided by the Plan's HIPAA Privacy Policies & Procedures, determines which employees are authorized to have access to ePHI to perform their job responsibilities.

   b. The Security Officer is responsible for supervising and limiting technical access to ePHI to only those employees who have been granted access to such information by the Security Officer.

      (i) Permission to access ePHI may not be inherited, rather it must be specifically granted.

      (ii) The Security Officer determines which employees have permission to access ePHI.

B. Workforce Clearance Procedure (Addressable). The Security Officer will use the Security Officer's judgement to determine those employees for which access to ePHI is necessary and appropriate. Specifically,

   1. The Privacy Officer (who is identified in the Plan's HIPAA Privacy Policies & Procedures) has the discretion to determine which employees need access to ePHI. This determination essentially is based on the employees' responsibilities.

   2. In making his/her determinations, the Security Officer limits access to ePHI to the minimum number of employees necessary, and trains and supervises the employees to ensure that ePHI is sufficiently protected and secure, and that its use and disclosure is appropriately limited. If an employee's ability to handle or maintain ePHI comes into question, the Security Officer shall take appropriate action.

C. Termination Procedures (Addressable). The Plan has implemented the following procedures for terminating access to ePHI when the employment of an employee ends or a Business Associate engagement terminates. When an employee or Business Associate is terminated, the Security Officer is immediately notified. Upon such notification, the Security Officer coordinates with the Plan's Business Associates to immediately terminate that employee's or Business Associate's physical and technical access to ePHI.

## IV. INFORMATION ACCESS MANAGEMENT

**POLICY:** Access to ePHI, which is consistent with the Plan's HIPAA Privacy Policies & Procedures, is authorized as follows.

A. Access authorization (Addressable). The Plan has delegated access authorization to a Business Associate. The Business Associate grants access to ePHI through permissions to access in the form of a username and password that can be used from any computer.

1. The Business Associate maintains overall responsibility for objectively managing security with the input of the Security Officer to determine who should have access to ePHI.

B. Access establishment and modification (Addressable). The procedure for establishing or modifying access to the Business Associate's network is as follows:

1. The Security Officer determines the need for that employee to access ePHI and reports that to the proper Business Associate. The Security Officer periodically reviews to determine if access must be modified based upon job function.

## V. SECURITY AWARENESS AND TRAINING

**POLICY:** The Security Officer conducts security awareness and training program for employees as appropriate and necessary for their job functions.

A. Security reminders (Addressable). The Security Officer provides training on HIPAA Security and will update training for affected employees if changes are made to the facilities or systems that create, receive or maintain ePHI. Security training is provided when an employee is on-boarded, on an annual basis and as needed when a security system or control is introduced. Security reminders are issued periodically.

B. Protection from malicious software (Addressable). The Security Officer ensures that each employee's computer has virus protection software and email security in place.

C. Log-in monitoring (Addressable). The Plan has delegated log-in monitoring to a third-party IT vendor and to its Business Associates. The Plan has implemented the following procedures for monitoring log-in attempts and reporting discrepancies.

1. After five unsuccessful attempts at logging in, the individual is automatically locked out of the system and a notification is sent to the Plan Sponsor's third-party vendor IT who may disable the account. Further Access Control measures are described in Policy IV, incorporated herein by reference. Log-in monitoring is conducted via single-sign-on. Inappropriate or attempted log-in is identified via active direct authentication.

2. These actions do not directly grant or revoke permissions relating to the locations in which ePHI is maintained, but rather, these actions are the best practices for protecting the environment where ePHI resides.

3. Passwords must have at least 16 characters, they expire after 12 weeks.

4. Two-factor authentication must be used to access Microsoft office 365, which includes access to email, e-file storage, and documents.

D. Training.

1. Employees to be Trained. Security training will be provided to the employees as is necessary and appropriate for those employees to carry out their job responsibilities.

2. Training Topics. Workforce security training shall include, but not be limited to, an overview of the HIPAA Security Standards, and an explanation of how the various employees' job responsibilities will be impacted by these Security Policies and Procedures.

3. Completion of Training and Documentation. Successful completion of initial and periodic training is a prerequisite for system access and a factor of job performance. The Security Officer will maintain a record for six (6) years documenting that the appropriate employees have fulfilled the training requirement.

## VI. SECURITY INCIDENT PROCEDURES

**POLICY:** The Plan addresses "security incidents" as described herein. Security incidents are defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

A. Response and Reporting (Required). The Plan has implemented the following procedures to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Plan; and document security incidents and their outcomes.

1. Identify and Respond.

a. Identify Threats.

(i) Technical Threats. The Plan Sponsor coordinates with Business Associates and third-party agents to identify and analyze events and incidents impacting the Plan Sponsor infrastructure/environment. The information is kept confidential, but Security Incidents are audited as part of continued audit requirements of the Plan's Business Associates in conjunction with annual SOX audits.

(ii) Physical Threats. If any employees observe a physical threat to ePHI, such as an unauthorized employee accessing ePHI, that observation is reported immediately to the Security Officer.

b. Once the Security Officer is made aware of the threat, based on the severity and impact of the threat, the incident response plan is activated to deal with the threat according to pre-established process and procedures outlined in the incident response plan.

c. Based on the incident report, the Security Officer performs a root cause analysis with regard to the possible security incident, and the Security Officer takes any necessary and appropriate remedial and/or disciplinary action to limit the immediate threat. In the Security Officer's discretion, the Security Officer may confer any other appropriate before taking any action in response to a security incident.

2. Mitigation. Based on the root cause analysis, the Security Officer uses the Security Officer's discretion to implement any remedial measures, including system improvements, process changes, immediate password changes, or additional training, that the Security Officer determines are necessary to protect against similar security incidents in the future.

3. Documentation. All security incidents initially will be documented and in incident reports. The Security Officer thereafter shall be responsible for documenting the root cause analysis of the security incident, and any remedial or disciplinary action taken in response to the security incident.

## VII. CONTINGENCY PLAN

**POLICY:** The Plan responds to emergencies and/or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that may damage systems that contain ePHI as described herein.

A. Data backup plan (Required). Data backup plan exists for the Plan Sponsor's systems.

1. The Plan Sponsor uses Microsoft 365 for all email communications and business document electronic storage. Plan personnel do not retain PHI in the physical Plan Sponsor office space. No paper files with PHI exist.

    a. Microsoft 365 is backed up continuously on Microsoft maintained servers.

    b. Cybersecurity professionals employ all appropriate resources to protect data and information stored continuously.

2. The Plan Sponsor office space is in a secure building co—located with the Radnor Police Station. The police department operates from the lower level and the Plan Sponsor's offices are located on the second floor.

    a. In the event of a physical disaster affecting the office space, all Plan Sponsor employees are prepared to work remotely. Each person's home office serves as a second office for the Plan Sponsor.

    b. The Plan Sponsor's procedures for redundancy require paper files to be scanned and stored in the Plan Sponsor's Microsoft 365 shared drive account.

    c. The use of LastPass, or some other secure password management system will allow Plan Sponsor employees to operate from any location or device. However, any new devices purchased or used for Plan Sponsor work must be enrolled in the remote monitoring system and set up with all cybersecurity preventative systems. The Plan Sponsor currently uses Endpoint Security.

    d. The Plan Sponsor's voice over IP telephone application is portable. Employees are not reliant on desk phones to make or receive phone calls and voicemail messages.

    e. The Security Officer will activate any contingency plans by communicating directly with staff via text, email, and/or phone. Staff may work remotely for as long as needed.

    f. Since all ePHI is stored in Business Associate systems, internet connections with our Business Associate systems will support access, reporting, and operating functions to continue.

    g. The contingency plan will unfold based upon situational issue identification and problem-solving.

        (i) The Security Officer will determine the status of the physical office to know if or when employees may return.

(ii) Daily communications with staff are ideal to provide reassurance and guidance during any interruptions of normal operations.

(iii) The Security Officer and Director of Marketing and Communications will work to notify Business Associates and vendors of the disruption. This notification will modify the mailing address, or other communication instructions, as needed.

h. This contingency plan should be reviewed in the following instances:

(i) Security Officer transition.

(ii) Every two years.

(iii) Following any incidents requiring contingency plan actions.

i. This Contingency Plan should be tested in a tabletop exercise annually, as part of a regular staff meeting.

3. All Plan data is stored remotely.

a. As noted above, the Plan Sponsor systems do not retain ePHI. HIPAA protected information is retained in Business Associate Systems and may be accessed on occasion, but Plan personnel should not prepare or store any data or reports containing ePHI.

b. Occasionally, the Plan is in receipt of ePHI via email between privacy employees. These limited instances are in the course of work related to benefit plan administration. The Plan uses Citrix Sharefile to transmit and receive any private or identifiable information.

c. Emails sent with any amount of ePHI must be encrypted. The Plan's email, when encrypted, is HIPAA compliant, and a Business Associate Agreement is in place with the email system provider.

d. Backup data is secured in Microsoft 365 Servers. These servers are regularly backed up remotely with multiple redundancies.

e. The Plan's information technology vendor will test, train, and ensure compliance with security policies. The Security Officer will also ensure compliance with these policies.

B. Disaster recovery plan (Required). Disaster recovery standards and guidelines exist for the Plan Sponsor's systems.

1. The Plan Sponsor does not store data and is therefore not responsible for restoring lost data. Business Associates must guarantee that lost data may be restored. The Executive Director and Benefits Consultants will work with Business Associates in the event an Associate loses data to ensure its prompt and accurate restoration.

C. Emergency mode operation plan (Required). To operate in emergency mode, the employees would access remotely the ePHI from anywhere via remote access software using two factor authentication and Plan Sponsor owned device.

D. Testing and revision procedures (Addressable). The Plan has different levels of contingency plans for the various systems and services, based on a number of factors.

1. The Plan will work with its Cybersecurity Insurance Carrier and Information Technology consultant to review cybersecurity policy and procedure annually.

2. In addition:

   a. The Plan will conduct regular and ongoing cybersecurity training awareness, including testing of employee awareness and behaviors.

   b. All employees will participate in regular training and testing.

   c. Contingency and security plans will be revised when:

      (i) Technology changes inform a need to modify plans

      (ii) Security Officer transition

      (iii) Regulations change

      (iv) The physical space, location, or some other variable changes.

   d. When changes are made to this policy, all employees will participate in formal training to increase awareness and comprehension of contingency plans.

E. Applications and data criticality analysis (Addressable). The Plan has assessed the relative criticality of specific applications and data in support of other contingency plan components, as follows: ePHI and email are both SaaS (Software as a Service) solutions. All backup and recovery procedures are handled by the relevant vendors. E-mail server is the highest priority system for recovery. Websites and ePHI are secondary for data criticality. All other systems are lower priority than these.

## VIII. EVALUATION

**POLICY:** The Plan shall perform periodic technical and nontechnical evaluations, based initially upon the implementation of these Security Policies and Procedures and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establish the extent to which the Plan's HIPAA Security Policies and Procedures meet the requirements of the Security Standards.

A. Evaluations.

1. Initial Evaluation. The Security Officer or his/her designee shall perform an initial technical and nontechnical evaluation based upon the Security Standards that establishes the extent to which these Security Policies and Procedures meet the requirements of the Security Standards.

2. Subsequent Evaluations. Any documentation related to cybersecurity is reviewed annually for completeness and accuracy. Technical controls are evaluated at least annually. The Security Officer or the Security Officer's designee shall perform periodic technical and nontechnical evaluations that establish the extent to which the Security Policies and Procedures meet the requirements of the Security Standards as follows:

   a. In response to environmental or operational changes affecting the security of ePHI; and

   b. Permissions for authorization to ePHI shall be audited yearly per business internal audit process.

## IX. BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

**POLICY:** The Plan has received the requisite satisfactory assurances from its business associates, in the form of written Business Associate Agreements, that the business associates will appropriately and reasonably safeguard the Plan's ePHI.

A. Business Associate Agreements (Required). The Business Associate Agreements between the Plan and its business associates have been amended in writing to provide that the Business Associate shall --

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Plan as required by the Security Standards;

2. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

3. Report to the Plan any security incident of which it becomes aware, including breached of unsecured PHI;

4. Authorize termination of the contract by the Plan, if the Plan determines that the business associate has violated a material term of the contract.

B. Standard Agreement. The Plan requires Business Associates to execute its standard Business Associate Agreement. Any deviation from this practice must be approved by the Privacy Officer.

C. Termination of Agreement. If the Plan learns or knows of a pattern of an activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the Business Associate Agreement, the Plan shall take reasonable steps to cure the breach or end the violation, as applicable. If such steps were unsuccessful, the Plan shall terminate the contract or arrangement.

## X. FACILITY ACCESS CONTROLS

**POLICY:** Physical access to the Plan's electronic information systems and facilities that house the Plan's ePHI is limited as described herein. These limitations protect the ePHI from unauthorized access while ensuring that properly authorized access is allowed.

A. Contingency operations (Addressable). In the event that the physical facilities that house Plan ePHI are inaccessible due to an emergency situation, the restoration of lost data under the disaster recovery plan and emergency mode operations plan will be achieved through the restoration of back-up files, which are stored at an off-site location operated by the Plan's Business Associate.

B. Facility security plan (Addressable); and Access Control and Validation Procedures (Addressable). The Plan has implemented the following Security Policies and Procedures to safeguard the facilities and the equipment that house ePHI from unauthorized physical access, tampering, and theft; and, to control and validate a person's access to the facilities based on their role or function, including visitor control and control of software programs for testing and review.

1. General Access. The Plan Sponsor does not maintain physical data centers on behalf of the Plan. Access to the Plan's data centers is delegated to the Plan's Business Associates and is tightly controlled.

    a. A combination of security cards, coded locks, and physical screening or authorizations are employed.

    b. Non- employees must be escorted through data centers.

2. Workstation Security.

    a. The workstations of Privacy Employees are configured to restrict access to those individuals who have a valid user ID and password.

    b. The Plan Sponsor's third-party IT vendor has administrative passwords that can access workstations.

3. Server Security. Server security is maintained by each Business Associate. The Trust does not maintain a server. Trust electronic files are stored in Microsoft 365. All member information is retained in Business Associate systems, all of which are password protected.

4. Maintenance records (Addressable). Repairs and modifications to the physical components of the office space/facilities where ePHI is housed are documented as follows.

    a. Repairs or modifications to the walls, doors, locks, and other physical elements of the office space/facilities where ePHI is housed are documented through facilities request forms which are maintained by the Plan Sponsor. The facilities request forms indicate the date of repair, the repair undertaken and reason for it, and the identity of the individual who performed the repair.

    b. Repairs or modifications to hardware are documented through tickets issued through the Plan Sponsor's third-party IT vendor. The vendor is responsible for responding to and maintaining these tickets. The tickets indicate the date of repair, the repair undertaken and the reason for it, and the identity of the individual who performed the repair.

## XI. WORKSTATION USE AND SECURITY

**POLICY:** The proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI is specified herein. In addition, the physical safeguards that restrict workstation access to authorized users are described herein.

A. Physical and Technical Safeguards:

1. Workstations timeout after five minutes of inactivity.

2. Employees who access ePHI through their workstations are required to lock their workstations when they leave their workstation for any amount of time.

3. During the establishment of new vendor partnerships, individuals are identified regarding who is authorized to have access to ePHI.

## XII. DEVICE AND MEDIA CONTROLS

**POLICY:** The receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility are handled as follows.

A. Disposal (Required). ePHI and/or the hardware or electronic media that stores that information is safely disposed of as follows:

1. The Plan generally does not maintain ePHI on the Plan Sponsor's hardware or electronic media. To the extent ePHI is maintained on the Plan Sponsor's hardware or electronic media, the Plan Sponsor employs procedures to destroy the contents of any such hardware or electronic media that is being retired from production.

2. Hard drives in all laptops are wiped clean using an approved method for overwriting the contents of such drives.

3. Mobile devices are wiped clean prior to being disposed of.

B. Media re-use (Required). Any computer that needs to be re-used, including those that contain or have access to ePHI, is re-formatted and re-imaged before it is put into alternative service. This process includes wiping the hard drive and reinstalling any applicable software from scratch.

C. Accountability (Addressable). Servers are not moved unless pre-approved for re-use or disposal by the Security Officer.

D. Data backup and storage (Addressable). When a server is upgraded or replaced, the Plan Sponsor's third-party IT vendor creates back-up tapes in order to create a retrievable, exact copy of the data on that server.

## XIII. ACCESS CONTROL

**POLICY:** Access to electronic information systems that maintain ePHI is limited to those persons that have been granted access rights. Further procedures are described in policies maintained by the Plan's Business Associates, incorporated herein by reference.

A. Unique user identification (Required). Each user who has access to the network system is assigned an account with a unique user identification and must establish his/her own unique password. Passwords must have at least 16 characters, they expire after 365 days, and the account is disabled after five (5) invalid attempts.

B. Emergency access procedure (Required). The procedure by which the employees can access and obtain the necessary ePHI during an emergency is set forth above in Policy VI (Contingency Plan).

C. Automatic logoff (Addressable). The electronic sessions of the employees who have access to ePHI are locked after five minutes of inactivity. These procedures are further described in policies maintained by the Plan's Business Associates.

D. Encryption and decryption (Addressable). Data levels above confidential classification are required to be encrypted. Further procedures are described in policies maintained by the Plan's Business Associates.

## XIV. AUDIT CONTROLS

**POLICY:** The Plan records and examines activity in information systems that contain or use ePHI. The Security Officer will conduct a cybersecurity audit every two years, or when a new business associate is selected as a vendor.

1. Business Associates must ensure risk-based audit controls over all information systems that contain or use ePHI

2. The Security Officer will conduct or outsource to a firm to conduct a cybersecurity audit with business associates to ensure auditing controls are in place to protect systems containing or using ePHI.

3. The systems and processes audited are detailed in the Cybersecurity Questionnaire, attached as Exhibit A to this policy.

## XV. INTEGRITY

**POLICY:** ePHI is protected from improper alteration or destruction.

A. Mechanism to authenticate electronic PHI (Addressable). The following electronic mechanisms corroborate that ePHI has not been altered or destroyed in an unauthorized manner:

1. Permissions are set up so that documents can only be modified, altered or deleted by the original author. If an employee needs or desires to modify, alter or delete a document that was created by someone else, that individual has to re-save the document under his/her authorship to make any such modifications.

2. Information received through the encrypted websites hosted by the Plan's business associates is protected from being modified during transmission by virtue of encryption.

## XVI. PERSON OR ENTITY AUTHENTICATION

**POLICY:** The Plan verifies that a person or entity seeking access to ePHI is the one claimed.

A. Verification on the Plan Sponsor's System: ePHI is not stored or saved on the Plan Sponsor's system.

B. Verification on the Business Associates' Websites**:** The Business Associate-sponsored websites that maintain encrypted TCP/IP mechanisms authenticate the user that is seeking ePHI through the web authentication processes.

## XVII. TRANSMISSION SECURITY

**POLICY:** The Plan has implemented technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

A. Integrity controls (Addressable) and Encryption (Addressable). Integrity controls and encryption are set forth in Policy XV and Policy XIII, incorporated herein by reference.

B. The Plan Sponsor uses Sharefile by Citrix for encrypted email and receipt of files with any member data. Sharefile by Citrix is a HIPAA compliant system for data transmission.

## XVIII. GROUP HEALTH PLAN REQUIREMENTS

**POLICY:** The Plan contains language providing that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the Plan Sponsor on behalf of the Plan.

A. The Plan contains provisions to require the plan sponsor to:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Plan;

2. Ensure that the adequate separation is supported by reasonable and appropriate security measures;

3. Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

4. Report to the group health plan any security incident of which it becomes aware.

## XIX. POLICIES AND PROCEDURES

**POLICY:** The Plan has implemented reasonable and appropriate Security Policies and Procedures to comply with the Security Standards or implementation specifications taking into account those factors specified in §164.306(b)(2).

A. Policies and Procedures. This document constitutes the Security Policies and Procedures of the Plan as required by the Security Standards. The Security Policies and Procedures implemented are, in the Plan's opinion, reasonable and appropriate and, to the best of the Plan's knowledge, compliant with the Security Standards.

B. Violations. This Policy is not to be construed to permit or excuse an action that violates any Security Standard, implementation specification, or other requirements of the Security Standards.

C. Amendments. The Plan may change these Security Policies and Procedures at any time, provided that the changes are documented and are implemented in accordance with the Security Standards.

## XX. DOCUMENTATION

**POLICY:** The Plan maintains documentation of these Security Policies and Procedures to comply with the Security Standards.

A. The Plan maintains these Security Policies and Procedures in written (which may be electronic) form; and

B. If an action, activity or assessment is required by the Security Standards to be documented, the Plan maintains a written (which may be electronic) record of the action, activity, or assessment.

1. Time limit (Required). The Plan will retain the documentation required by paragraph (B) of this Policy for at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

2. Availability (Required). The Plan will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

3. Updates (Required). The Security Officer will review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.