<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>HIPAA Privacy and Security Policies &amp; Procedures Overview (Policy &amp; Procedure)</td>
</tr>
<tr>
<td>2.</td>
<td>[Reserved]</td>
</tr>
<tr>
<td>3.</td>
<td>Administrative Safeguards</td>
</tr>
<tr>
<td>3-1</td>
<td>Assigned Security Responsibility</td>
</tr>
<tr>
<td>3-2</td>
<td>Security Management Process</td>
</tr>
<tr>
<td>3-3</td>
<td>Workforce Security</td>
</tr>
<tr>
<td>3-4</td>
<td>Information Access Management</td>
</tr>
<tr>
<td>3-5</td>
<td>Security and Awareness Training</td>
</tr>
<tr>
<td>3-6</td>
<td>Security Incident Procedures</td>
</tr>
<tr>
<td>3-7</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>3-8</td>
<td>Evaluation</td>
</tr>
<tr>
<td>3-9</td>
<td>Business Associate Contracts and Other Arrangements</td>
</tr>
<tr>
<td>4.</td>
<td>Technical Safeguards</td>
</tr>
<tr>
<td>4-1</td>
<td>Access Control</td>
</tr>
<tr>
<td>4-2</td>
<td>Audit Control</td>
</tr>
<tr>
<td>4-3</td>
<td>Integrity</td>
</tr>
<tr>
<td>4-4</td>
<td>Personal or Entity Authentication</td>
</tr>
<tr>
<td>4-5</td>
<td>Transmission Security</td>
</tr>
<tr>
<td>5.</td>
<td>Physical Safeguards</td>
</tr>
<tr>
<td>5-1</td>
<td>Facility Access Controls</td>
</tr>
<tr>
<td>5-2</td>
<td>Workstation Use</td>
</tr>
<tr>
<td>5-3</td>
<td>Workstation Security</td>
</tr>
<tr>
<td>5-4</td>
<td>Device and Media Controls</td>
</tr>
</tbody>
</table>
HIPAA Security Policies and Procedures Overview

Policy Statement
HIPAA requires covered entities to have policies and procedures reflecting HIPAA's security mandates. The Health Plan, as a covered entity, has developed administrative policies and procedures reflecting the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations.

Policy Interpretation and Implementation

HIPAA Policies and Procedures
1. HIPAA requires covered entities to have policies and procedures to ensure compliance with HIPAA's regulations. A health plan is a "covered entity" under HIPAA. Consequently, the Health Plan is responsible for the research, development, implementation, monitoring and maintenance of the Health Plan's HIPAA security policies and procedures regarding electronic protected health information (ePHI).

Health Plan
2. HIPAA defines a "health plan" as an individual or group health plan that provides or pays the cost of medical care, including, but not limited to, employee welfare benefit plans covered by ERISA, health insurers, HMOs, group health plans, and many public benefit programs (Medicaid, Medicare, etc.).

Organized Health Care Arrangement (OHCA)
3. HIPAA recognizes Organized Health Care Arrangements (OHCA). An OHCA can exist when an employer sponsors more than one health plan that is a covered entity. Being part of an OHCA allows the covered entities to satisfy the HIPAA privacy and security requirements together, as if they are a single covered entity. The following covered entities are designated as an OHCA:
   - Hopkins School District 270 Group Medical Plan
   - Hopkins School District 270 Health Reimbursement Arrangement
   - Hopkins School District 270 Employee Assistance Plan
   - Hopkins School District 270 Health Care Expense Reimbursement Plan

4. For purposes of these HIPAA policies and procedures, "Health Plan" means the OHCA designated above.

5. For purposes of these HIPAA policies and procedures, "Plan Sponsor" means the Hopkins School District, the sponsor of the health plans that are part of the OHCA.

Work Together
6. The policies and procedures prepared for purposes of HIPAA Privacy compliance and the policies and procedures prepared for purposes of HIPAA Security compliance are intended to work together.
Definition of Protected Health Information (PHI)

7. Protected Health Information (PHI) means individually identifiable information relating to:
   a. The past, present or future physical or mental health or condition of an individual;
   b. The provision of health care to an individual;
   c. The past, present or future payment for health care provided to an individual.

Definition of Electronic Protected Health Information (ePHI)

8. Electronic Protected Health Information (ePHI) means PHI maintained or transmitted in electronic media, including, but not limited to, electronic storage media (i.e., hard drives, digital memory medium) and transmission media used to exchange information in electronic storage media (i.e., internet, extranet, and other networks). PHI transmitted via facsimile and telephone is not considered to be transmissions via electronic media.

Revisions to HIPAA Policies and Procedures

9. The Health Plan’s HIPAA policies and procedures may be revised at any time, in order to comply or enhance compliance with HIPAA.

Policy Inquiries

10. Inquiries relative to HIPAA policies and procedures should be directed to the HIPAA Security Officer.

Specific Policies and Procedures

11. The Health Plan’s specific policies and procedures, as reflected in this document, have been created in order to satisfy HIPAA’s security requirements.

   The Health Plan has no employees. All of the Health Plan’s functions, including creation and maintenance of its records, are carried out by employees of the Plan Sponsor and by business associates of the Health Plan. The Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit ePHI, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Plan Sponsor and business associates. Accordingly, the employees of the Plan Sponsor and business associates create, receive, maintain, and transmit all of the ePHI relating to the Health Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit ePHI relating to the Health Plan, and control their employees, agents, and subcontractors who have access to ePHI relating to the Health Plan. The Health Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI relating to the Health Plan. That ability lies solely with the Plan Sponsor and business associates.

   Because the Health Plan has no direct access to or control over the employees, equipment, media, facilities, policies,
procedures, or documentation of its business associates; and because the business associates have undertaken certain obligations relating to the security of ePHI that they handle in relation to the performance of administrative functions for the Health Plan, the Health Plan hereby adopts and incorporates by reference the business associates’ HIPAA security policies and procedures with respect to the ePHI handled by such business associates. With respect to ePHI handled by the Plan Sponsor on behalf of the Health Plan, the HIPAA security policies and procedures reflected in this document apply.

Other Laws

12. In addition to HIPAA, covered entities may be subject to other laws that address the privacy and/or security of health information, including, but not limited to, the Minnesota Data Practices Act. HIPAA establishes a floor – the minimum requirements with which a covered entity must comply. To the extent the requirements of any other law provide more protection to the subject of the health information, those requirements will apply.

Third Party Service Providers

13. Nothing precludes the Health Plan from contracting with a third party service for assistance in complying with the Health Plan’s HIPAA policies and procedures.

Record Retention

14. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer

15. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations


Effective Date


References:
45 C.F.R. § 164.530, 45 C.F.R. § 164.306.
[Reserved]

Policy Statement

Policy Interpretation and Implementation

1. 

2. 

3. 

4. 

5. 

6. 

7. 

8. 

9. 

10. 

References:
### Administrative Safeguards - Generally

#### Policy Statement
The Administrative Safeguards portion of the Security Rule (collectively referred to as "Administrative Safeguards") addresses administrative measures and the policy and procedures for their use that protect ePHI and control access to it. It includes administrative actions, and policies and procedures, to manage the selection of measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

#### Policy Interpretation and Implementation

<table>
<thead>
<tr>
<th>Standards and Implementation Specifications</th>
<th>1. The Administrative Safeguards portion of the Security Rules consists of nine standards. Some of these standards in turn include implementation specifications designed to further the standard.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach</td>
<td>2. The Health Plan must consider, evaluate, and document its assessment, including recommendations for improvement.</td>
</tr>
<tr>
<td>Coordination with Privacy Policies and Procedures</td>
<td>3. The Administrative Safeguards standards apply in addition to the HIPAA privacy policies and procedures where the PHI involved is ePHI.</td>
</tr>
<tr>
<td>Definition of Protected Health Information (PHI)</td>
<td>4. Protected Health Information (PHI) means individually identifiable information relating to:</td>
</tr>
<tr>
<td></td>
<td>a. The past, present or future physical or mental health or condition of an individual;</td>
</tr>
<tr>
<td></td>
<td>b. The provision of health care to an individual;</td>
</tr>
<tr>
<td></td>
<td>c. The past, present or future payment for health care provided to an individual.</td>
</tr>
<tr>
<td>Definition of Electronic Protected Health Information (ePHI)</td>
<td>5. Electronic Protected Health Information (ePHI) means PHI maintained or transmitted in electronic media, including, but not limited to, electronic storage media (i.e., hard drives, digital memory medium) and transmission media used to exchange information in electronic storage media (i.e., internet, intranet, and other networks). PHI transmitted via facsimile and telephone is not considered to be transmissions via electronic media.</td>
</tr>
<tr>
<td>Record Retention</td>
<td>6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.</td>
</tr>
<tr>
<td>HIPAA Security Officer</td>
<td>7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any</td>
</tr>
</tbody>
</table>

Form 3 – Administrative Safeguards (Policy & Procedure)
questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be
directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except
holidays at 952-988-4103.

8. Violations of the HIPAA Security Policies and Procedures
shall be subject to discipline.


References:
45 C.F.R. § 164.308
Assigned Security Responsibility
[Administrative Safeguard]

Standard
A Security Officer must be identified and shall be responsible for the development and implementation of the Security Policies and Procedures.

Interpretation and Implementation Specifications

Appointment of HIPAA Security Officer

1. The Health Plan has appointed the Director of Technology of the Hopkins School District 270 as the Health Plan's HIPAA Security Officer.

HIPAA Security Officer's Responsibilities

2. The HIPAA Security Officer's responsibilities include:
   a. Assisting management in the development, implementation, and updating of the Health Plan's HIPAA policies and procedures;
   b. Performing periodic security risk assessments;
   c. Development of security procedures and guidelines for the protection of the Health Plan's information systems;
   d. Assisting management in the assigning of passwords and user identification codes for access to electronic protected health information (ePHI) by authorized users;
   e. Assisting in the development of training materials and training to ensure that relevant staff are well trained in matters relating to the protection and safeguarding of ePHI;
   f. Providing staff, individuals, business associates, and government agencies with information regarding the Health Plan's HIPAA policies and procedures; and
   g. Working with the Health Plan's legal counsel on matters relative to HIPAA.

Delegation

3. The HIPAA Security Officer may delegate certain job functions to be performed by other individuals; however, the ultimate responsibility for compliance with HIPAA remains with the HIPAA Security Officer.

Relationship to Privacy Officer

4. The HIPAA Security Officer can be, but is not required to be, the same individual as the HIPAA Privacy Officer. Should the HIPAA Security Officer be a different individual than the HIPAA Privacy Officer, the HIPAA Privacy Officer has overall responsibility for protected health information (PHI), including electronic protected health information (ePHI).
General HIPAA Requirements

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer

6. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

7. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.308(a)(2).
Security Management Process
[Administrative Safeguard]

Standard
The Health Plan must implement policies and procedures to prevent, detect, contain, and correct security violations.

Interpretation and Implementation Specifications

Risk Analysis
(required)
1. The Health Plan shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity. For this purpose, "held by" includes ePHI that is housed other than by the Health Plan (e.g., third party administrators).

Risk Management
(required)
2. The Health Plan shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA’s security requirements.

Workforce Sanctions
(required)
3. The Health Plan shall apply appropriate sanctions against workforce members who fail to comply with these Security Policies & Procedures. The Discipline Policy contained in the Hopkins School District 270 Organized Healthcare Arrangement HIPAA Privacy Policies & Procedures and Administrative Forms shall apply with respect to violations of these Security Policies & Procedures.

Information System Activity Review
(required)
4. The Health Plan has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. The Health Plan keeps track of all ticket records, using key words to alert further investigation. Security Policies & Procedures shall be reviewed annually as well as upon any breach.

General HIPAA Requirements

Record Retention
5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
6. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of
ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

7. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.


References:
45 C.F.R. §§ 164.308(a)(1)(i).
Workforce Security
[Administrative Safeguard]

Standard
The Health Plan shall implement policies and procedures designed to provide access to those with a recognized need for access to ePHI and preclude access to those without such a recognized need.

Interpretation and Implementation Specifications

Authorization and/or Supervision (addressable)
1. The Health Plan has implemented procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Only the Plan Sponsor's employee benefits specialists are authorized to access ePHI. Such employees are subject to the supervision of the Privacy Officer.

Workforce Clearance Procedures (addressable)
2. The Health Plan has implemented procedures to determine when and under what circumstances the access of a workforce member to ePHI is appropriate. Only the Plan Sponsor's employee benefits specialists are authorized to access ePHI. Access is allowed only for purposes described in the Health Plan's HIPAA Privacy Policies & Procedures. Workforce clearance shall be reviewed annually and upon any breaches in policy.

Termination Procedures (addressable)
3. The Health Plan has implemented procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made in the Workforce Clearance Procedure. The Assistant Superintendent shall notify business associates to terminate access of workforce members or former workforce members who are no longer authorized to access ePHI. The Security Officer shall terminate access of such individual's to the Plan Sponsor's information systems by notifying the Plan Sponsor's IT Department that access should be terminated. The IT Department will then terminate all access and directory services for the user's account.

General HIPAA Requirements

Record Retention
4. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any
questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

6. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.308(a)(3)(i).
Information Access Management
[Administrative Safeguard]

Standard
The Health Plan shall implement policies and procedures for authorizing access to ePHI.

Interpretation and Implementation Specifications

Access Authorization
(addressable)

1. The Health Plan shall implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism. Access to ePHI shall be available only through a password protected computer. EPHI is stored in a protected folder on the Plan Sponsor's server that only authorized employees have the ability to access via a password protected employee management/payroll system.

Access Establishment and Modification
(addressable)

2. The Health Plan has implemented policies and procedures that, based upon the access authorization policies described above, establish, document, review, and modify a user's right of access to a workstation, transaction, program, process, or other mechanism. User rights are established first by their role. For users that require additional access based upon their role, the user's supervisor, in this case the Security Officer, details the additional access rights required in a ticket to the Plan Sponsor's IT Department. All requests for additional access rights are reviewed by the Technology Director before the additional access rights are granted. Standard user security applies, under no circumstances will secure data be held anywhere other than on the district server.

General HIPAA Requirements

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer

4. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.
Violations

5. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.308(a)(4)(i).
Security and Awareness Training
[Administrative Safeguard]

Standard
The Health Plan shall implement a security awareness and training program for all new and existing members of its workforce (including management). In addition, periodic re-training should be conducted when operational, environmental, or other key factors change and such change impacts the security of ePHI. The Health Plan has established a HIPAA training program pursuant to its HIPAA Privacy Policies & Procedures. Such training program will address security awareness and training.

Interpretation and Implementation Specifications

Workforce Members
1. An employee/workforce member, for the purposes of this policy, means any employee, trainee, volunteer, or any other person(s) whose conduct, in the performance of work for the Health Plan, is under the direct control/supervision of the Health Plan, regardless of payment source.

Security Reminders
(addressable)
2. The Health Plan shall conduct periodic security updates. These updates will be included in the periodic training updates described in the Health Plan's HIPAA Privacy Policies & Procedures.

Protection from Malicious Software
(addressable)
3. The Health Plan has established procedures for guarding against, detecting, and reporting malicious software. The Health Plan uses vulnerability scanning software.

Log-in Monitoring
(addressable)
4. The Health Plan has established procedures for monitoring log-in attempts and reporting discrepancies. The HIPAA Security Officer is alerted when anyone has attempted to log into the Plan Sponsor's information systems more than 5 times.

Password Management
(addressable)
5. The Health Plan has established procedures for creating, changing, and safeguarding passwords. Passwords are created using a unique combination of letters, numbers and characters. Passwords must be at least 8 characters, at least one upper case, one lower case, one letter and one special character. Passwords are to be changed every 90 days. Passwords are kept in a password protected spreadsheet in the benefits folder accessible only to the benefits coordinator on the password protected server.

General HIPAA Requirements

Record Retention
6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.
7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

8. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Security Incident Procedures
[Administrative Safeguard]

Standard
The Health Plan shall implement policies and procedures to address "security incidents," including how to identify security incidents and require reporting of such a security incident to the appropriate person(s).

Interpretation and Implementation Specifications

Definition of "security incident"
1. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Response and Reporting (addressable)
2. The Health Plan shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. The Health Plan follows the Minnesota Government Data Practices Act under Minnesota Statutes, chapter 13.

General HIPAA Requirements

Record Retention
3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
4. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
5. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.308(a)(6)(i).
## Contingency Planning  
[Administrative Safeguard]

### Standard
The Health Plan shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

### Interpretation and Implementation Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Backup Plan (required)</td>
<td>1. The Health Plan has established and implemented procedures to create and maintain retrievable exact copies of ePHI. Such procedures are described in the Plan Sponsor’s Disaster Recovery Plan, which is incorporated herein by reference.</td>
</tr>
<tr>
<td>Disaster Recovery Plan (required)</td>
<td>2. The Health Plan has established and implemented procedures to restore any loss of data. Such procedures are described in the Plan Sponsor’s Disaster Recovery Plan, which is incorporated herein by reference.</td>
</tr>
<tr>
<td>Emergency Mode Operation Plan (required)</td>
<td>3. The Health Plan has established and implemented procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Such procedures are described in the Plan Sponsor’s Disaster Recovery Plan, which is incorporated herein by reference.</td>
</tr>
<tr>
<td>Testing and Revision Procedures (addressable)</td>
<td>4. The Health Plan has implemented procedures for periodic testing and revision of contingency plans. Such procedures are described in the Plan Sponsor’s Disaster Recovery Plan, which is incorporated herein by reference.</td>
</tr>
<tr>
<td>Applications and Data Criticality Analysis (addressable)</td>
<td>5. The Health Plan shall assess the relative criticality of specific applications and data in support of other contingency plan components.</td>
</tr>
</tbody>
</table>

### General HIPAA Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Retention</td>
<td>6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.</td>
</tr>
</tbody>
</table>

**HIPAA Security Officer**

7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular
business office hours Monday through Friday, except holidays at 952-968-4103.

8. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.


References:
45 C.F.R. § 164.308(a)(7).
Evaluation
[Administrative Safeguard]

Standard
The Health Plan shall perform initial and periodic technical and non-technical evaluations of compliance (required to establish extent to which security policies and procedures meet requirements).

Interpretation and Implementation Specifications

Evaluation
1. The Health Plan will conduct periodic, routine reviews and evaluations of these HIPAA Security Policies & Procedures to ensure they meet the requirements of the HIPAA security rule. Also, these HIPAA Security Policies & Procedures will be reviewed and evaluated as soon as administratively practical after the Health Plan or Plan Sponsor makes any environmental or operational changes that affect the security of ePHI.

General HIPAA Requirements

Record Retention
2. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
3. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
4. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.308(a)(8).
Business Associate Contracts and Other Arrangements
[Administrative Safeguard]

Standard
The Health Plan shall obtain satisfactory assurances that the business associate will appropriately safeguard ePHI before permitting the business associate to create, receive, maintain, or transmit ePHI.

Interpretation and Implementation Specifications

Definition of “business associate”
1. A business associate, means a person or entity who is not an employee or workforce member of the Health Plan, who performs or assists in the performance of a function or activity on behalf of the Health Plan that involves the use or disclosure of PHI, or provides legal, actuarial, accounting, consulting, data compilation, management, administrative, accreditation, or financial services.

Identification of Business Associates
2. It is the Health Plan’s obligation to ensure that all of the Health Plan’s business associates have a written valid business associate agreement. The Security Officer will identify all business associates of the Health Plan.

Written Contract or Other Arrangement (required)
3. The Health Plan will require all business associates to enter a written business associate agreement that meets the applicable requirements of § 45 C.F.R. § 164.31(a).

General HIPAA Requirements

Record Retention
4. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
6. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.308(b).
Technical Safeguards - Generally

Policy Statement
The Technical Safeguards portion of the Security Rule (collectively referred to as "Technical Safeguards") addresses technology and requires policy and procedures for its use that protect ePHI and control access to it.

Policy Interpretation and Implementation

Standards and Implementation Specifications

1. The Technical Safeguards portion of the Security Rules consists of five standards:
   - Access Control,
   - Audit Control,
   - Integrity,
   - Personal or Entity Authentication, and

   Some of these standards in turn include implementation specifications designed to further the standard.

Approach

2. The Health Plan must consider, evaluate, and document its assessment, including recommendations for improvement.

Coordination with Privacy Policies and Procedures

3. The Technical Safeguards apply in addition to the HIPAA privacy policies and procedures where the PHI involved is ePHI.

General HIPAA Requirements

Record Retention

4. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

6. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.312.
Access Control
[Technical Safeguard]

Standard
The Health Plan shall implement technical procedures to restrict access to electronic information systems maintaining ePHI to allow access only to authorized persons and/or software programs.

Interpretation and Implementation Specifications

"Access" Defined
1. "The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."

Electronic Information Systems
2. The policies and procedures implemented under this standard take into account all of the Health Plan's electronic information systems used to maintain and access ePHI, including, but not limited to, computer servers (local and remote or cloud-based), desktop computers, laptop computers, hand-held devices (e.g., smart phones), home computers, etc. Currently, the Plan Sponsor maintains ePHI solely on a local computer server. Access to such server is allowed only through desktop computers located on the Plan Sponsor's premises and through off premises computers through an encrypted terminal services gateway.

Unique User Identification (required)
3. The Health Plan assigns a unique name and/or number for identifying and tracking user identity.

Emergency Access Procedure (required)
4. The Health Plan has established and implemented procedures for obtaining necessary ePHI during an emergency. The administrator in charge of managing the emergency shall contact the benefits coordinator and make a direct request for the specific information needed to manage the situation.

Automatic Logoff (addressable)
5. The Health Plan has implemented electronic procedures that terminate an electronic session after 5 minutes of inactivity.

Encryption and Decryption (addressable)
6. The Health Plan has determined, based upon its risk analysis, that it is unnecessary to encrypt ePHI maintained by the Plan Sponsor.

"Encryption"
7. A method of converting regular text into coded text.

General HIPAA Requirements

Record Retention
8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
9. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any
questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

10. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.312(a)
Audit Control
[Technical Safeguard]

Standard
The Health Plan shall implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI.

Interpretation and Implementation Specifications

Audit Control
1. The Health Plan shall track all access logs of our software programs as well as data held on the server.

General HIPAA Requirements

Record Retention
2. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
3. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
4. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.312(b).
Integrity
[Technical Safeguard]

Standard
The Health Plan shall implement policies and procedures to protect ePHI from improper alteration or destruction.

Interpretation and Implementation Specifications

Mechanism to Authenticate
ePHI
(required)

1. The Health Plan has implemented electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. Access to the software systems is limited to solely the benefits administrator. All data is backed up on a secure location in our data center. The Plan Sponsor monitors data integrity through file metadata.

General HIPAA Requirements

Record Retention

2. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer

3. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

4. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date


References:
45 C.F.R. § 164.312(c)(i).
Personal or Entity Authentication
[Technical Safeguard]

Standard
The Health Plan shall implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Interpretation and Implementation Specifications

Personal or Entity Authentication
1. The Plan Sponsor assigns unique passwords to all employees authorized to access ePHI. The Plan Sponsor’s computer system grants access to ePHI only if an authorized password is used. Employees with access to ePHI are prohibited from sharing their passwords with any other person without specific authority from the HIPAA Security Officer.

General HIPAA Requirements

Record Retention
2. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
3. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
4. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.312(d).
Transmission Security
[Technical Safeguard]

**Standard**
The Health Plan shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic transmission network.

**Interpretation and Implementation Specifications**

"Electronic transmission network"

- 1. Includes e-mail, Internet, and private or point to point networks.

**Integrity Controls** (addressable)

- 2. The Health Plan has implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. The Plan Sponsor's email system is password protected. Emails sent by the Plan Sponsor containing ePHI are sent with password-protected access.

**Encryption** (addressable)

- 3. The Health Plan has determined, based upon its risk analysis, that it is unnecessary to encrypt ePHI that is transmitted by the Plan Sponsor.

"Encryption"

- 4. A method of converting regular text into coded text.

**General HIPAA Requirements**

**Record Retention**

- 5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

**HIPAA Security Officer**

- 6. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

**Violations**

- 7. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

**Effective Date**


**References:**

45 C.F.R. § 164.312(e)(1).
Physical Safeguards - Generally

Policy Statement
The Physical Safeguards portion of the Security Rule (collectively referred to as "Physical Safeguards") provide additional protection of ePHI. Physical safeguards are defined as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Policy Interpretation and Implementation

Standards and Implementation Specifications
1. The Physical Safeguards portion of the Security Rules consists of four standards. Some of these standards in turn include implementation specifications designed to further the standard.

Approach
2. The Health Plan must consider, evaluate, and document its assessment, including recommendations for improvement.

Coordination with Privacy Policies and Procedures
3. The Physical Safeguards standards apply in addition to the HIPAA privacy policies and procedures where the PHI involved is ePHI.

General HIPAA Requirements

Record Retention
4. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
6. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.310(a).
Facility Access Controls  
[Physical Safeguard]

**Standard**
The Health Plan shall implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

**Interpretation and Implementation Specifications**

<table>
<thead>
<tr>
<th>Contingency Operations (addressable)</th>
<th>1. The Health Plan has established and implemented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Security Plan (addressable)</td>
<td>2. The Health Plan has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Key card access is required to enter the building in which the applicable equipment is located. The office in which such equipment is located shall be kept locked when not occupied.</td>
</tr>
<tr>
<td>Access Control and Validation Procedures (addressable)</td>
<td>3. The Health Plan has implemented policies and procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. The Plan Sponsor uses badge access to data centers to confirm identity, layered security, and keyed door access.</td>
</tr>
<tr>
<td>Maintenance Records (addressable)</td>
<td>4. The Health Plan has implemented policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, wall, doors and locks).</td>
</tr>
</tbody>
</table>

**General HIPAA Requirements**

| Record Retention | 5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both. |
| HIPAA Security Officer | 6. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies |
and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations

Effective Date

7. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.


References:
45 C.F.R. § 164.312(a)(1).
Workstation Use
[Physical Safeguard]

Standard
The Health Plan shall to specify the functions of, manner in which functions are to be performed by, and physical attributes of workstations with access to ePHI.

Interpretation and Implementation Specifications

Workstation Defined
1. "An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."

Workstation Use
2. Users shall follow the Plan Sponsor's Acceptable Use Policy, including the rule prohibiting the use of personal devices for work functions. The Acceptable Use Policy is incorporated herein by reference.

General HIPAA Requirements

Record Retention
3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
4. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
5. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

Effective Date

References:
45 C.F.R. § 164.310(b).
Workstation Security
[Physical Safeguard]

**Standard**
The Health Plan shall implement physical safeguards for all workstations that access ePHI and to restrict access to authorized users.

**Interpretation and Implementation Specifications**

**Workstation Defined**
1. "An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."

**Workstation Security**
2. Key card access is required to enter the building in which the applicable workstations are located. The office in which such workstations are located shall be kept locked when not occupied.

**General HIPAA Requirements**

**Record Retention**
3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

**HIPAA Security Officer**
4. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

**Violations**
5. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.

**Effective Date**

**References:**
45 C.F.R. § 164.310(c).
Device and Media Controls
[Physical Safeguard]

Standard
The Health Plan shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.

Interpretation and Implementation Specifications

Disposal
(required)
1. The Health Plan has implemented policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. If a server will be disposed, ePHI contained on such server will be erased using appropriate software.

Media Re-use
(required)
2. The Health Plan has implemented procedures for removal of ePHI from electronic media before the media are made available for re-use. If a server will be moved and used for a different purpose, ePHI contained on such server will be erased using appropriate software.

Accountability
(addressable)
3. The Health Plan shall maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Data Backup and Storage
(addressable)
4. The Health Plan shall create a retrievable, exact copy of ePHI, when needed, before movement of equipment. The Plan Sponsor’s computer systems are generally backed up locally on servers.

General HIPAA Requirements

Record Retention
5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Security Officer
6. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 952-988-4103.

Violations
7. Violations of the HIPAA Security Policies and Procedures shall be subject to discipline.
Effective Date


References:
45 C.F.R. § 164.310(d)(1).