ILLINOIS EDUCATORS RISK MANAGEMENT PROGRAM GROUP HEALTH PLAN

SECURITY POLICY MANUAL

TABLE OF CONTENTS

Subject: Purpose of Security Policy Manual

Reference: 42 USC. 1320d – 1320d-8
45 CFR 164.302 – 164.316

The purpose of this Security Policy Manual is to develop and implement the policies and procedures necessary to enable the Plan referenced on the title page ("Plan") as well as the Illinois Educators Risk Management Program Association as plan sponsor of the Plan ("Plan Sponsor" or "Employer"), to comply with the requirements of the Security Rule. 45 CFR 164.103 et seq.

The policies defined in this guide apply to all board members, officers, employees, and agents of the Employer. This policy guide supersedes all prior relevant policy statements or informal practices.

This guide provides privacy and security policy information for board members, officers, employees, management personnel and agents. It provides added details to help the Employer's board members, officers, employees, and agents to safeguard privacy and security of electronic protected health information.

The Employer is a dynamic and evolving organizations operating in a competitive and changing business and technological environment. Because of this, these policies are under continual review. New policies may be developed or policies may be changed at any time based upon the needs of the Plan.

All policy information contained in this policy manual is intended to be in compliance with relevant laws and regulations. Policies are developed unilaterally by management and are not intended to guarantee employment security or specific benefits, nor to be interpreted as any form of contract.

Employees, supervisors, managers, board members, officers, and agents are expected to administer policies and benefits within the guidelines of these policies. The Security Official must authorize any exceptions to this policy.

This guide shall apply to Health Alliance, except that Health Alliance may use its own forms and security policies and procedures provided such forms, policies and procedures comply with the HIPAA privacy rule and security rule.

The Employer shall have the right to interpret the intent of this Security Policy Manual. The Security Officer and all other Employer's personnel involved in Plan operations shall comply with and enforce the Security Policy Manual as interpreted by the Employer.

Information System Security Standards

Reference: 45 CFR 164.306

POLICY: It is the policy of the Plan to develop and implement information system security policies and procedures related to protecting the privacy and security of protected health information.

PROCEDURE:

1. The Plan is committed to managing its information system in a manner which achieves the objectives listed below. It is the Plan's objective:

- to ensure the confidentiality, integrity and availability of all electronic protected health information which is created, received, maintained or transmitted in the course of providing health care services;

- to protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

- to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under Privacy Rule regulations;

- to ensure that the Plan's personnel perform tasks in compliance with HIPAA security standards.

2. The Employer will use those security measures that allow the Plan to reasonably and appropriately implement privacy and security standards as defined in 45 CFR 164.302- 164.318.

3. The Plan measures will consider organizational size and complexity, technical infrastructure and computer capabilities, costs, and degree of risks to integrity of protected health information in the Plan's possession.

4. As required by the HIPAA Security standard, the Plan's security policies and procedures will address the following areas:

Administrative Safeguards
Physical Safeguards
Technical Safeguards
Organizational Requirements
Policies and Procedures

5. As specified by the HIPAA Security Standard, certain **Required** actions will be implemented. Additionally, certain **Addressable** actions will be assessed and implemented as reasonable and appropriate. In the event that an addressable action is not implemented, such action shall be documented, identifying reason(s) for not taking such action and identifying other equivalent alternatives implemented.

6. Responsibility for implementation of the information system security safeguards is defined in the Administrative Safeguards policy.

7. Security measures will be reviewed and modified as needed to insure a reasonable maintenance of the security plan.

Administrative Safeguards

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to develop administrative safeguards as needed to develop a security management process complying with the HIPAA Security Standard.

PROCEDURE:

1. The Plan designates Lori Eisenmenger as the Security Officer, responsible for the development and implementation of the security management process.

2. The Security Officer is responsible to implement the following "Required" security management activities:

   a) Conduct a Risk Analysis. The risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of protected health information held by the Plan in electronic form. Risk Analysis is documented on the Risk Analysis checklist.

   b) Risk Management. Risk management is the development and implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

   c) Sanction Policy. A sanction policy shall be defined and communicated to all personnel. The sanction policy defines sanctions or other corrective or disciplinary action which will be taken against violators to enforce the security policies.

   d) Information System Activity Review. The information system activity review consists of procedural guidelines and actions for the periodic review of the organization's information system. A systems review includes review of systems records such as audit logs, access reports, and security incident tracking reports.

3. The Security Officer is responsible to develop and use checklists, reports or other records to document the administrative safeguards taken.

4. Administrative safeguards shall be reviewed annually and modified as needed.

5. In the event that the security management process identifies shortcomings, the Security Officer is responsible to develop plans and implement procedures to correct the shortcomings to reduce risks and vulnerabilities to a reasonable and appropriate level.

Information Access Management

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to develop and implement policies and procedures related to controlling access to protected health information.

PROCEDURE:

1. The Security Officer is responsible to develop procedures for the control of access to electronic protected health information. Such access shall be based on job functions, responsibilities and system controls.

2. The following classes of persons are permitted to use or access protected health information depending on their job responsibility. Use or access is permitted as listed below:

Job Class	Purpose or Justification
Plan Sponsor Board Members	To supervise and manage the Plan
Plan Sponsor Executive Board Members	To supervise and manage the Plan
Plan Sponsor Officers	To supervise and manage the Plan
Plan Administrator Officers	To supervise and manage the Plan

3. Other Employer's personnel shall be given access to protected health information only incident to and necessary for their assistance in administering the Plan.

4. Access to protected health information by other personnel is limited to the specific job related purpose of the work activity being performed. System design, password controls, and system screen access shall be limited to job activities or functions performed.

5. The respective department or functional supervisor is responsible to identify individuals permitted to gain access, provide access instructions or procedures, and to supervise work activities to assure that access instructions are complied with.

6. In the event that an individual changes jobs or if job responsibilities change eliminating the defined justification for access to protected health information, the supervisor is responsible to notify the Security Officer. The Security Officer is responsible for taking action prevent further access by such individual to protected health information.

7. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Authorization Procedure for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop and implement policies and procedures related to defining and limiting authorization to access protected health information.

PROCEDURE:

1. The Security Officer is responsible to develop procedures for the defining and limiting authorization to access protected health information. Such access shall be based on job functions, responsibilities and system controls.

2. The following classes of persons within the organization are permitted to use or access protected health information depending on their job responsibility. Use or access is permitted as listed below:

Job Class	Work activity	Access Level
Plan Sponsor Board Members	To Supervise and Manage the Plan	Full Access
Plan Sponsor Executive Board Members	To Supervise and Manage the Plan	Full Access
Plan Sponsor Officers	To Supervise and Manage the Plan	Full Access
Plan Administrator Officers	To Supervise and Manage the Plan	Full Access

3. Access to protected health information by other personnel is limited to the specific job related purpose of the work activity being performed. Password controls and system screen access are defined based on access limits correlated to job activities or functions performed.

4. The respective department or functional supervisor is responsible to identify individuals permitted to gain access, specify access level, provide access instructions or procedures, and to supervise work activities to assure that access instructions are complied with.

5. In the event that an individual changes jobs or if job responsibilities change eliminating the defined justification for access to protected health information, the supervisor is responsible

to notify the Security Officer. The Security Officer is responsible for taking action to prevent further access by such individual to protected health information

6. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Workforce Clearance Procedure for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop and implement policies and procedures related to defining and permitting clearance for access to protected health information.

PROCEDURE:

1. The Security Officer is responsible to develop procedures related to defining and permitting clearance for access protected health information. Such clearance shall define levels of access and system controls based on job functions and responsibilities.

2. The classes of persons within the organization permitted to use or access protected health information depending on their job responsibility is defined in the policy on Authorization Procedure for Protected Health Information.

3. Access to protected health information by other personnel is limited to the specific job related purpose of the work activity being performed. Password controls and system screen access are defined based on access limits correlated to job activities or functions performed as defined below:

   a) Verify current employment or organizational status of individual

   b) Review job description of individual

   c) Refer to the Authorization Procedure for Protected Health Information to confirm job categories authorized for access

   d) Designate department or functional log in code which limits access level

   e) Designate individual password

4. Access levels are defined as summarized below:

Access Level	Definition
Level 0	Not eligible for access to protected health information.
Level I	Able to view selected screens or data based on job function. May print data to pre-defined reports.

Level II	Able to view selected screens, enter data, and print reports based on job function.
Level III	Able to view selected screens, enter data, change or correct data, sort data and print reports based on supervisory role for job function.
Level IV	Authorized access to multiple data base sectors based on management role able to view selected screens, enter data, change or correct data, sort data and print reports
Level V	Authorized access to all system data base sectors based on management role able to view selected screens, enter data, change or correct data, sort data and print reports
Level VI	Authorized access to programs, code and system controls to design and maintain system. Authorized access to all system data base sectors for system design/maintenance or management role

4. The respective department or functional supervisor is responsible to provide access instructions or procedures, and to supervise work activities to assure that access instructions are complied with.

5. In the event that an individual changes jobs or if job responsibilities change eliminating the defined justification for access to protected health information, the supervisor is responsible to notify the Security Officer. The Security Officer is responsible for taking action to prevent further access by such individual to protected health information. See Access Termination Procedure.

6. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Access Termination Procedure for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop and implement policies and procedures related to termination of access to protected health information.

PROCEDURE:

1. The Security Officer is responsible to oversee procedures related to terminating access to protected health information. Such access and termination of access shall be based on job functions and responsibilities.

2. The respective department or functional supervisor is responsible to supervise work activities to assure that access instructions are followed. In the event that an individual changes jobs or if a job responsibilities change eliminating the defined justification for access to protected health information, action shall be taken to prevent further access by such individual to protected health information

3. When a job change occurs as defined above, the respective department or functional supervisor is responsible to notify the Security Officer that the individual's access is terminated. Termination of access shall include the following actions:

   a) Document new employment or organizational status of individual.

   b) System adjustment to modify or block use of individual's password and log-in code.

   c) Re-assignment of tasks performed by individual now terminated from access.

   d) Notification of affected individuals or departments relating to re-assignment of responsibilities.

4. The respective department or functional supervisor responsible to supervise work activities is accountable to review departmental computer files or other operating records to check for any unauthorized use or disclosure of data. Any unauthorized use or disclosure incidents shall be reported to the Security Officer.

5. The Security Officer is responsible to review system audit logs and trails to check for any unauthorized use or disclosure of data. Any unauthorized uses or disclosures incidents shall be reported to the Privacy Officer and/or other designated superior.

6. In the event of any unauthorized use or disclosure, for which an accountable individual is identified, see Sanction Policy.

Access Authorization Procedure for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop an access authorization procedure permitting clearance for access protected health information.

PROCEDURE:

1. The Security Officer is responsible to oversee procedures related to defining and granting access authorization to protected health information.

2. Access to protected health information by the Employer's personnel is limited to the specific job related purpose of the work activity being performed. The respective department or functional supervisor is responsible to identify individuals eligible for access to protected health information and to specify level of access. (See Workforce Clearance Procedure for Protected Health Information.)

3. The respective department or functional supervisor is responsible to verify current employment or organizational status of individual confirming that the individual is an active employee or other authorized individual. This is documented on a Request for Access to PHI form.

4. The respective department or functional supervisor is responsible to review job description and/or job assignment of individual and to document responsibility by providing a current job description and list of current job tasks relating to access to protected health information.

5. The employee or individual may designate his/her preferred password, subject to guidelines defined by the Security Officer.

6. The respective department or functional supervisor is responsible to refer to the Authorization Procedure for Protected Health Information to confirm job categories authorized for access and to specify the level of access granted to the individual being authorized.

7. Upon receipt of the Request for Access to PHI form, the Security Officer is responsible to designate department or functional log in code which limits access level.

8. The Security Officer then sets system controls to accept the log-in code and password. In the event of any compatibility problem related to a requested password, the Security Officer shall instruct the individual on selecting another appropriate password.

9. The Security Officer is responsible to establish a random and/or planned time schedule for changing log-in codes and passwords. Such instructions shall be communicated to affected employees as needed.

10. The Security Officer is responsible to periodically verify a user's right to access and to assure compliance with security policies and procedures.

11. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Changes to Access Authorization for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop an access authorization procedure permitting clearance for access protected health information and to define guidelines for handling changes to access authorization.

PROCEDURE:

1. The Security Officer is responsible to oversee procedures related to defining and granting access authorization to protected health information and for responding to changes to access.

2. Access to protected health information by authorized personnel is limited to the specific job related purpose of the work activity being performed. The respective department or functional supervisor is responsible to identify individuals eligible for access to protected health information and to specify level of access. In the event of job or employment status changes affecting authorization for access, the respective department or functional supervisor is responsible to take action as defined in this procedure. (Also see Workforce Clearance Procedure for Protected Health Information.)

3. The respective department or functional supervisor is responsible to verify current employment or organizational status of individual confirming that the individual is an active employee or other authorized individual. This is documented on a Request for Access to PHI form. In the event that the change results in termination of access, see Access Termination Procedure.

4. The respective department or functional supervisor is responsible to review job description and/or job assignment of individual and to document responsibility by providing a current job description and list of current job tasks relating to access to protected health information. In the event of a change in job duties or responsibilities, such change may affect access authorization or level of authorization.

5. The respective department or functional supervisor is responsible to refer to the Authorization Procedure for Protected Health Information to confirm job categories authorized for access and to specify the new level of access granted to the individual being authorized as a result of the change.

6. A new password shall be defined when there is a change in access status. The employee may designate his/her preferred password, subject to guidelines defined by the Security Officer.

7. Upon receipt of the Request for Access to PHI form, the Security Officer is responsible to designate department or functional log in code which changes or limits access level as appropriate.

8. The Security Officer then sets system controls to accept the log-in code and password. In the event of any compatibility problem related to a requested password, the Security Officer shall instruct the employee on selecting another appropriate password.

9. The Security Officer is responsible to establish a random and/or planned time schedule for changing log-in codes and passwords. Such instructions shall be communicated to affected employees as needed.

10. The Security Officer is responsible to periodically verify a user's right to access and to assure compliance with security policies and procedures.

11. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Security Awareness and Training Program

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop and implement a security awareness and training program.

PROCEDURE:

1. The Security Officer is responsible to develop and implement a security awareness and training program. The training materials shall include, but not be limited to, access to a copy of this Security Policy Manual.

2. Training shall be provided for all members of the workforce including management who are involved in the operation of the Plan.

3. Training shall be conducted:

- no later than the compliance date for the security rule;
- for each new employee hired or other authorized individual involved with the Plan subsequent to the compliance date;
- for each employee or other authorized individual whose functions or responsibilities change, resulting in access to protected health information;
- following any change in policies or procedures relating to HIPAA privacy or security requirements or changes to the HIPAA security rule or related regulations.

4. The Security Officer or other designated individual is responsible to maintain a record of training provided pursuant to this policy. Training records may be in document or electronic form. A sample training acknowledgment is attached to this policy.

Security Awareness and Prevention Procedures

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop and implement a security awareness and prevention procedures.

PROCEDURE:

1. The Security Officer is responsible to develop and implement one or more security awareness and prevention activities as outlined in this policy.

2. The Security Officer shall develop and disseminate periodic security procedure updates as appropriate to communicate revisions to security policies.

3. The Security Officer shall take steps to provide protection from malicious software. Examples are listed below:

   a) Install virus check software to system network, conduct periodic virus checks, require downloads only with approval and subject to virus check, and periodically update virus definitions.

   b) Advise individuals that any software installations including screen savers are subject to approval of the Security Officer and will be checked for virus or conflicts with existing applications.

   c) Approve changes in program files.

   d) Advise individuals that all e-mails are subject to virus check.

4. The Security Officer shall establish procedures and system controls to monitor log-ins including:

   a) Maintain a record of log-in attempts, noting source terminal of attempt, date, time, and attempted log-in code.

   b) Investigation taken as needed in the event of questionable log-in attempts.

5. The Security Officer shall establish procedures and system controls to track, control and monitor password use.

   a) Individuals shall be instructed in recommended ways to define a password, and precautions to safeguard the password.

b) Passwords shall be changed at periodic intervals.

6. Incidents identified by these procedures shall be recorded as defined in the Incident procedure.

7. An individual's disregard or failure to follow access procedures or an unauthorized access or disclosure shall result in corrective action as defined in the Sanction Policy.

Verification of Access Authorization for Protected Health Information

Reference: 45 CFR 164.308 (Addressable)

POLICY: It is the policy of the Plan to develop procedures for verification of access authorization to audit access to protected health information and to assure that only authorized individuals are gaining access.

PROCEDURE:

1. The Security Officer is responsible to oversee procedures related to defining and granting access authorization, and to audit work practices to assure that only authorized individuals are actually accessing protected health information. See procedures on workforce clearance and access authorization for guidelines on defining which employees have access to protected health information.

2. The Security Officer is responsible to establish periodic audits and checks to verify a user's right to access and to assure compliance with security policies and procedures. Examples of audits may include one or more of the following:

- Track of password(s) or other ID used to log onto protected health information system
- Track of password(s) or other ID used when entering transactions within the protected health information system
- Audit comparison of password or other ID corresponding to individual, workstation, or work activity
- Audit comparison of password or other ID corresponding to assigned clearance level, or work function
- Establishment and audit of periodic system pause requiring re-entry of password or log - on code(s)
- Production of one or more reports to document audit activity.

3. The Security Officer is responsible to establish administrative guidelines for use by a department supervisor or work group leader to conduct periodic audits or checks to verify a user's right to access and to assure compliance with security policies and procedures.

Examples of audits may include one or more of the following:

- Establishment of periodic audit procedures to be conducted by the supervisor to verify use of proper password or log - on code(s)

- Production of one or more reports to document audit activity.

4. The respective department or functional supervisor is responsible to periodically review the list of individuals eligible for access to protected health information and to verify level of access. In the event of duty or employment status changes affecting authorization for access, the respective department or functional supervisor is responsible to take action as defined in this procedure.

- Verify current employment or organizational status of individual confirming that the individual is an active employee or other authorized individual. In the event that the change results in termination of access, see Access Termination Procedure.

- The respective department or functional supervisor is responsible to review and verify task description and/or task assignment of individual. In the event of a change in duties or responsibilities, such change shall be evaluated for its affect upon access authorization or level of authorization.

- The respective department or functional supervisor is responsible to review and verify work activity of the individual. In the event of a change in work activity such change shall be evaluated for its affect upon access authorization or level of authorization.

5. The respective department or functional supervisor is responsible to prepare a Request for Access to PHI form to document any change of status relating clearance or access authorization to protected health information.

6. Upon receipt of the Request for Access to PHI form, the Security Officer is responsible to maintain a department or functional log in code which documents changes or limits access level as appropriate.

7. The Security Officer then sets or adjusts system controls to accept or prohibit the log-in code and password.

8. The Security Officer is responsible to establish a random and/or planned time schedule for changing log-in codes and passwords. Such instructions shall be communicated to affected employees as needed.

9. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Security Incident Procedures

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to develop and implement a security incident procedures to guide proper and timely response to any security incident.

PROCEDURE:

1. The Security Officer is responsible to develop and implement one or more security incident procedures as outlined in this policy.

2. The Security Officer shall develop and make available a security incident report form with instructions for use by individuals to report security incidents.

3. Individuals shall be instructed on recognizing common security incidents and advised on how to respond to such incidents. Examples of security incidents may include one or more of the following:

- actual or attempted theft of records, data, or system equipment
- actual or attempted access to records, data, or system equipment by an individual who is not authorized for such access
- actual or attempted disclosure of records, data, or system security controls by an individual who is not authorized to make such disclosures or such disclosures are made to unauthorized persons.
- actual or attempted damage to or destruction of records, data, or system equipment.
- accidental disclosure or damage or destruction to records, data, or system equipment or other incident causing actual or attempted disclosure or damage or destruction of records, data, or system equipment.

4. In the event of any incident as described in paragraph 3 above, the employee shall immediately report the incident to his/her department or functional supervisor. The incident shall be documented on an Incident report. The department or functional supervisor is responsible to report the incident to the Security Officer.

5. The Security Officer shall conduct an internal investigation into the incident. As necessary, the Security Officer may confer with the Privacy Officer, department supervisor, or other personnel to determine an appropriate course of action.

6. The Security Officer shall respond to suspected or known security incidents and take action to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity.

7. The security incident and follow-up activity shall be documented to detail corrective action taken.

8. An individual's disregard or failure to follow access procedures or unauthorized access or disclosure shall result in corrective actions as defined in the Sanction Policy.

Data Security Contingency Plan

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to develop and implement a data security contingency plan to guide proper and timely response to any emergency such as fire, vandalism, system failure, natural disaster or other security incident.

PROCEDURE:

1. The Security Officer is responsible to develop and implement a required data security contingency plan as outlined in this policy to the extent any electronic protected health information is maintained.

2. The data security plan shall consist of the following required components and may contain certain addressable components:

- Data Backup Plan (required)
- Disaster Recovery Plan (required)
- Emergency Mode Operation Plan (required)
- Testing and revision procedures (addressable)
- Applications and data criticality analysis (addressable)

3. The Data Backup Plan shall consist of the following elements:

- Daily and weekly backups of electronic health information shall be performed.
- A full system backup shall be scheduled each weekend.
- Data shall be stored on backup media, marked as backup, and dated.
- Backup media shall be stored off-site at a location designated by the Security Officer.
- Appropriate security safeguards shall be observed to protect against unauthorized use, disclosure, or other loss of backup data.
- The medical records clerk shall maintain a log of backup activities.

4. The Disaster Recovery Plan shall consist of the following elements:

- Backup media (including the operating system, applications, and data) shall be maintained at a separate off-site location as designated by the Security Officer.

- In the event of a disaster incident, the following recovery plan shall be implemented as directed by the Security Officer and defined in the Emergency Mode Operation Plan.

5. The Emergency Mode Operation Plan shall consist of the following elements:

- Acquire necessary resources to perform a restore of computer system and medical applications.

- System backups shall be restored for use in providing the Plan services.

- Staff shall provide regular services to the extent possible based on availability of suitable facilities, equipment and personnel.

- Facilities and/or equipment shall be restored as quickly as possible.

6. The Security Officer is responsible to develop and implement any procedures as necessary for testing and revision of data security contingency plans. Revisions may occur as a result of new equipment, technologies, office relocations, personnel changes or experiences in implementing the contingency plan. The Security Officer shall confer with others as needed to test and revise policies and procedures to accomplish this objective.

7. The Security Officer is responsible to develop and implement any procedures as necessary to assess the relative criticality of specific applications and data in support of the contingency plan components. Applications used in maintenance of medical records, billing, and accounting are determined to be critical to Plan operations.

The following contingencies shall be made:

- Arrangements shall be made with a system vendor for emergency replacement of damaged hardware.

- Backup media (including the operating system, applications, and data) maintained at a separate off-site location shall be loaded onto the replacement system.

8. The Security Officer is responsible to develop revised policies and procedures as necessary reflecting any revisions to the data security contingency plans.

Evaluation of Data Security Contingency Plan

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to periodically evaluate the extent to which security policies and procedures meet the requirements of the HIPAA Security Rule.

PROCEDURE:

1. The Security Officer is responsible to periodically evaluate the extent to which security policies and procedures meet the requirements of the HIPAA Security Rule.

During this evaluation, consideration shall be given to:

- HIPAA security regulations & requirements
- Adequacy of the Plan's security policies in addressing issues defined by the regulation
- Review of any security incidents
- Review of any privacy complaints
- Review of any unauthorized disclosures
- Consideration of any environmental or operational changes occurring since the Plan's security policy was initially implemented.
- Consideration of technical and non-technical issues

2. To accomplish this objective, the Security Officer shall confer with others as needed to evaluate policies and procedures to accomplish this objective.

3. An evaluation checklist may be used to document the evaluation process.

4. The Security Officer is responsible to develop and implement any new or revised procedures as necessary. Revisions may occur as a result of new equipment, technologies, office relocations, personnel changes or experiences in implementing the privacy security policies.

Security Requirements for Business Associates

Reference: 45 CFR 164.308 and 164.314 (Required)

POLICY: It is the policy of the Plan, when Business Associates are used to handle protected health information, to obtain a written agreement with the Business Associate organization to assure that the Business Associate exercises proper care to protect the privacy and security of protected health information.

PROCEDURE:

1. The Security Officer is responsible for ensuring that any Business Associate shall be permitted to create, receive, maintain or transmit electronic protected health information on behalf of the Plan only upon receipt of satisfactory assurances that the business associate will safeguard protected health information in accordance with requirements for the HIPAA security regulation.

2. A Business Associate is defined as:

   - A person or entity who provides certain activities, functions or services to or on behalf of the Plan involving use or handling or disclosure of protected health information, or

   - A healthcare provider or other entity covered by the privacy rule.

3. The Security Officer is responsible to insure that service arrangements between the Plan and the Business Associate are detailed in a contract, including assurances that the Business Associate will safeguard protected health information in accordance with requirements for the HIPAA security regulation, including assurances that it will:

   - implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of protected health information that it handles on behalf of the Plan;

   - ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect the information;

   - report to the covered entity any security incident of which it becomes aware; and

   - authorize termination of the contract if the covered entity determines that the business associate has violated a material term of the contract.

4. The Security Officer is responsible to monitor work activity related to electronic protected health information and that business associates are satisfactorily performing contracted services.

5. While the Plan is not required by HIPAA to actively monitor or oversee how protected health information safeguards are carried out, the Security Officer is responsible for exercising reasonable oversight to ensure that contracted services are performed as specified.

- In the event that the Plan becomes aware of any breach or violation of the service contract by the Business Associate, the Security Officer is responsible to take reasonable steps to cure any breach or end the violation.

- Such steps may include one or more of the following:

    1. Discuss needed service improvements

    2. Request changes in service or actions to correct service breach or violation

    3. Negotiate or re-negotiate service activities

    4. Delay, defer or withhold payment for services improperly performed

    5. Request or require documentation or proof of services rendered or other similar action to ensure that services are rendered as contracted.

- In the event that the Business Associate fails to remedy the breach or violation following reasonable efforts by the Plan to resolve the problem, the Security Officer may authorize termination of the agreement if feasible and subject to the terms of the agreement.

- In the event that termination of a service agreement is not feasible, the Security Officer is responsible to report the problem to the Department of Health and Human Services, Office for Civil Rights.

Security Requirements for Group Health Plan

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to limit disclosure of protected health information as defined by the Medical Privacy Rule and to ensure that Plan documents require the Plan sponsor to reasonably and appropriately safeguard electronic protected health information created, received maintained or transmitted to or by the Plan sponsor on behalf of the Plan.

PROCEDURE:

1. The Plan Sponsor is responsible to ensure that Plan documents of the Plan are amended to incorporate provisions to require the Plan Sponsor to implement privacy and security safeguards required by HIPAA.

2. Plan documents must be amended to address the following :

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that the Plan sponsor creates, receives, maintains, or transmits on behalf of the Plan;

- Ensure that the adequate separation required by HIPAA is supported by reasonable and appropriate security measures;

- Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and report to the Plan any security incident of which it becomes aware.

3. The Security Officer is responsible to prepare communications and instructions to the Plan personnel responsible to implement this policy through contacts with the Plan sponsor.

4. The Security Officer is responsible to establish reasonable controls to monitor the implementation of HIPAA required Plan amendments.

Facility Access Controls

Reference: 45 CFR 164.310 (Addressable)

POLICY: It is the policy of the Plan to establish facility access control 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.

PROCEDURE:

1. The Security Officer is responsible to establish facility access control 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.

2. Facility access controls may consist of one or more of the following action plans or control procedures.

- Contingency operations -- Development of 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.

- Facility Security Plan -- Development of policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

- Access controls and validation procedures -- Development of 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.

- Maintenance Records -- Development of policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (ie: computer hardware, walls, doors, locks, and power supply systems.

3. The foregoing list of facilities control action plans are considered addressable under HIPAA. To ensure compliance, the Security Officer is responsible to evaluate the need for such plan(s) as it relates to Plan operations, and then develop and implement such plan(s) as needed to provide reasonable safeguards of electronic protected health information.

4. In the event that the Security Officer determines that such plan(s) are not needed to safeguard information, such determination shall be documented identifying consideration of alternative solutions providing comparable protections.

5. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Guidelines for Workstation Use

Reference: 45 CFR 164.310 (Required)

POLICY: It is the policy of the Plan to establish guidelines for workstation use to promote reasonable security and safeguards in the handling of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to establish guidelines for workstation use to promote reasonable security and safeguards in the handling of electronic protected health information. These guidelines shall specify proper equipment operation procedures, functions to be performed, and the physical attributes of the surroundings of the workstation. The guidelines focus on defining reasonable controls for workstations that can access electronic protected health information.

2. The Security Officer is responsible to advise and instruct department or functional supervisors on proper set-up, use, and security safeguards relating to use of computer workstations.

3. Set up and operation of a computer workstation must comply with the following guidelines:

- Only computer terminals, lap tops and peripheral equipment authorized by the Security Officer may be connected to the Plan information system

- Only software or application programs authorized by the Security Officer may be installed or loaded onto the Plan information system and /or terminals.

- Only designated individuals assigned to work functions relating to electronic protected health information may operate computer terminals, software or systems dedicated to handling such information.

- Computer terminals shall be secured to workstations in a manner prescribed by the Security Officer.

- Computer terminals in areas where individuals work multiple shifts shall be adapted with a locking devise to prevent unauthorized access after regular working hours.

- Computer terminals shall be positioned to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals shall maintain a screen saver feature as authorized by the Security Officer to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals unavoidably positioned in an area where there are passers-by shall be fitted with a viewing filter as specified by the Security Officer to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals used for entering or handling electronic protected health information shall be segregated into a special area, partitioned area or office to separate this activity from other non-HIPAA regulated information processing.

4. Individuals performing authorized tasks involving use or disclosure of protected health information shall observe the following privacy and security practices:

- Do not share or disclose a personal password or log-on code with others.

- Do not access a secure data base in the presence of non-authorized persons.

- Do not leave your work area without first exiting the software application that handles protected health information.

- Be alert for any unusual incidents or unauthorized use or disclosure of protected health information and report such incident(s) to your supervisor.

- Do not copy or download protected health information data except as authorized.

- Do not copy or download applications programs or software.

- Do not install other programs or software onto the Plan's computer systems unless authorized.

5. The department or functional supervisor is responsible to implement the specified security procedures within their respective work area and to train individuals on proper use and security safeguards relating to operation of computer workstations.

6. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Guidelines for Workstation Security

Reference: 45 CFR 164.310 (Required)

POLICY: It is the policy of the Plan to establish guidelines for workstation security to promote reasonable security and safeguards for equipment and systems used in the handling of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to establish guidelines for workstation security to promote reasonable safeguards for equipment and systems used in the handling of electronic protected health information. These guidelines shall specify proper security precautions to protect systems and equipment. The guidelines focus on defining reasonable controls for workstations that can access electronic protected health information.

2. The Security Officer is responsible to advise and instruct department or functional supervisors on proper set-up, use, and security safeguards relating to use of computer workstations.

3. Set up and operation of a computer workstation must comply with the following guidelines:

- Only computer terminals, lap tops and peripheral equipment authorized by the Security Officer may be connected to the Plan's information system

- Computer terminals shall be secured to workstations in a manner prescribed by the Security Officer.

- Computer terminals in areas where employees work multiple shifts shall be adapted with a locking devise to prevent unauthorized access after regular working hours.

- Access controls, such as locked or controlled access work areas shall be used to prevent access by unauthorized persons and to verify proper access of individuals working in the work area.

- Surveillance or other work area monitoring systems shall be used as deemed appropriated by the Security Officer.

4. The department or functional supervisor is responsible to implement the specified security procedures within their respective work area and to train individuals on proper use and security safeguards relating to operation of computer workstations.

5. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Guidelines for Device and Media Controls

Reference: 45 CFR 164.310 (Required)

POLICY: It is the policy of the Plan to establish guidelines for workstation security to promote reasonable security and safeguards for device and media systems used in the handling of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to establish guidelines to promote reasonable safeguards for device and media systems used in the handling of electronic protected health information. These guidelines shall specify proper security precautions to protect device and media systems and equipment. The guidelines focus on defining reasonable controls for device and media systems that contain or can access electronic protected health information.

2. The Security Officer is responsible to advise and instruct department or functional supervisors on proper set-up, use, and security safeguards relating to use of device and media systems.

3. Set up and operation of a device and media systems must comply with the following guidelines:

- Only device and media systems authorized by the Security Officer may be connected to the Plan's information system.

- Device and media systems equipment shall be stored and secured in a manner prescribed by the Security Officer.

- Device and media systems in areas where employees work multiple shifts shall be adapted with a locking device to prevent unauthorized access or use after regular working hours.

- Access controls, such as locked or controlled access work areas shall be used to prevent access to device and media systems by unauthorized individuals and to verify proper access of employees working in the work area.

- Device and media systems may not be removed, altered, tampered with, or repaired except as authorized by the Security Officer.

- Surveillance or other work area monitoring systems shall be used as deemed appropriate by the Security Officer.

4. The department or functional supervisor is responsible to implement the specified security procedures within their respective work area and to train employees on proper use and security safeguards relating to operation of device and media systems.

5. The Security Officer is responsible to define disposal guidelines for media and devices, a HIPAA required action. The Security Officer is responsible to oversee disposal of media or devices according to the following guidelines:

- The Security Officer is responsible to determine which hardware device(s) and/or software media are subject to disposal.

- The respective department or functional supervisor is responsible to determine what information, data or electronic protected health information is contained on the media or device subject to disposal and to evaluate whether such data shall be retained or subject to disposal.

- Arrangements shall be made for transfer or copying of any data to be retained, providing appropriate safeguards to protect data confidentiality.

- Arrangement shall be made to erase, re-format or otherwise destroy data on any media or device subject to disposal.

6. The Security Officer is responsible to define re-use guidelines for media and devices, a HIPAA required action. The Security Officer is responsible to oversee re-use of media or devices according to the following guidelines:

- The Security Officer is responsible to determine which hardware device(s) and/or software media are subject to re-use.

- The respective department or functional supervisor is responsible to determine what information, data or electronic protected health information is contained on the media or device subject to re-use and to evaluate whether such data shall be retained or subject to disposal.

- Arrangements shall be made for transfer or copying of any data to be retained, providing appropriate safeguards to protect data confidentiality.

- Arrangement shall be made to erase, re-format or otherwise destroy data on any media or device subject to re-use.

- The data destruction action shall be documented, and certified by the individual(s) performing such task.

7. The Security Officer is responsible to determine whether there is a need to maintain a record of the movements of hardware and electronic media and any person responsible therefore,

a HIPAA addressable activity. Where the need is determined, a record or log of equipment assignments shall be maintained by the Security Officer or designee.

8. The Security Officer is responsible to determine whether there is a need to create a retrievable exact copy of electronic protected health information before movement of equipment. Where the need is determined, such copies shall be made by the Security Officer or designee.

9. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan's operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Technical Safeguards for Access Control

Reference: 45 CFR 164.312 (Required)

POLICY: It is the policy of the Plan to implement technical policies and procedures for electronic information systems that maintain electronic health information to allow access only to those persons or software programs that have been granted access due to their responsibility and function.

PROCEDURE:

1. The Security Officer is responsible to develop and implement technical policies and procedures for electronic information systems that maintain electronic health information to allow access only to those persons or software programs that have been granted access due to their responsibility and function.

2. The Security Officer is responsible to implement the following plan for a unique user identification, a required HIPAA safeguard. The plan shall consist of the following elements:

- Assign a unique name and/or number for each user.

- Set up system controls to display and/or track the unique identifier when the user logs onto the system.

- Set up system controls to display and/or track the unique identifier when the user makes any entries, or transactions within the system.

- Set up system controls to report discrepancies in use of name or number correlated to user.

3. The Security Officer is responsible to implement the following procedures for obtaining necessary electronic protected health information during an emergency. The procedures shall consist of the following elements:

- Back-up power -- identification of back-up power sources to prevent power interruption,

- Reduced service -- definition of reduced service level operations, permitting continuation of minimum essential operations in an emergency,

- Alternative or back-up computer system available for switchover,

- Backup storage of data or media available for access in an emergency,

- Contingency operations -- Development of 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.

- Master key access -- Development of System operator master key access to operating system or data to troubleshoot, resolve problems, and expedite emergency operations.

4. The Security Officer is responsible to determine whether there is a need for selected addressable technical safeguards, including automatic log off, encryption and decryption, and to implement such features if needed.

- Automatic log off (addressable) -- Development of electronic procedures that terminate an electronic session after a predetermined time of inactivity.

- Encryption and decryption (addressable) Development of a mechanism to encrypt and decrypt electronic protected health information.

5. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Audit Control Technical Safeguards

Reference: 45 CFR 164.312 (Required)

POLICY: It is the policy of the Plan to implement technical audit control policies and procedures for electronic information systems that maintain electronic health information to record and examine system activity.

PROCEDURE:

1. The Security Officer is responsible to implement technical audit control policies and procedures for electronic information systems that maintain electronic health information to record and examine system activity. Control actions or procedures may focus on audit of system hardware, software, or procedural mechanisms.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems that maintain electronic health information and to develop audit systems that reasonably and appropriately audit and track system use and access.

3. Examples of a system hardware audit system may include:

   - periodic inspection of system hardware components
   - inventory of system hardware components and periodic verification of components
   - Listing of location and use of hardware components and periodic verification
   - Use of inventory tags and periodic verification of inventory
   - Listing of assignment of hardware components to individual users and periodic verification
   - Specification of wiring connection to system hardware components and periodic verification

4. Examples of a system software audit system may include:

   - periodic inspection and testing of system software components
   - inventory of system software components and periodic verification of components
   - Listing of location and use of software components and periodic verification

- Listing of accessibility to software components by individual users and periodic verification

- Specification of system software access to specified work stations or work functions and periodic verification

- Specification of levels of system software access to specified work stations or work functions and periodic verification

5. The Security Officer is responsible to document audit controls through definition of written audit checklist defining audit steps, accountabilities, recording results and reporting discrepancies.

6. The Security Officer is responsible to establish an audit schedule and to conduct periodic audits on a random and/or scheduled basis.

7. In the event that the audit identifies any discrepancies, policy violations, or unauthorized access or use or disclosure of protected health information, the Security Officer is responsible to:

- Take action to stop or mitigate unauthorized access, use or disclosure of protected health information.

- Take action as appropriate under the Sanction Policy against any individual who violated privacy or security policies of the organization

8. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Technical Safeguards to Protect Data Integrity

Reference: 45 CFR 164.312 (Addressable)

POLICY: It is the policy of the Plan to implement technical safeguards to protect data integrity of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to implement technical safeguards to protect data integrity of electronic protected health information. Data integrity safeguards may focus on audit of system hardware, software, or procedural mechanisms.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems that maintain electronic health information and to develop data integrity procedures that reasonably and appropriately safeguard data.

3. Examples of a system hardware integrity safeguards may include:

   - Periodic inspection of system hardware components
   - Installation of emergency or back-up power supply units or systems preventing power loss affecting data integrity
   - Installation of power surge protectors to prevent or minimize equipment damage affecting data integrity
   - Installation of "firewall" or similar electro-mechanical systems designed to block and/or detect unauthorized access or damage by malicious software.
   - Evaluation and specification of hardware components to assure compatibility preventing clashes affecting data integrity

4. Examples of a system software integrity safeguards may include:

   - periodic inspection and testing of system software components
   - Installation of "crash guard" or similar software preventing software clashes or crashes affecting data integrity
   - Installation of encryption and decryption software to protect data security and to minimize damage affecting data integrity

- Installation of "firewall" or similar software systems designed to block and/or detect unauthorized access or damage by malicious software.

- Evaluation and specification of software components to assure compatibility preventing clashes affecting data integrity.

- Installation of access control software or procedures to prevent unauthorized access and to minimize damage affecting data integrity

5. The Security Officer is responsible to document technical safeguards to protect data integrity through definition of written procedures defining procedural steps, accountabilities, recording results and reporting discrepancies.

6. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Technical Safeguards for Data Authentication

Reference: 45 CFR 164.312 (Addressable)

POLICY: It is the policy of the Plan to implement technical safeguards for authentication of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to implement technical safeguards for authentication of electronic protected health information.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems and to identify methods and procedures for authentication of electronic protected health information.

3. The Security Officer may confer with the management of health care providers, health care clearing houses, government agencies, business associates and others to establish electronic data interchange procedures, systems, protocols, and methods of authentication of data received from or sent to such organizations or entities.

4. The Security Officer is responsible to implement mechanisms to authenticate electronic protected health information. Such mechanisms shall corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. Data integrity mechanisms may include one or more of the following:

- Electronic file comparison
- Electronic file comparisons before and after transmission
- File size counts, tracking and comparison
- File access tracking and reporting
- Scheduled and random integrity checks.

5. Examples of methods and procedures for authentication of electronic protected health information may include:

- periodic inspection and testing of system software components
- verification and authentication of access transactions or procedures to prevent unauthorized access

- verification, authentication matching of passwords, log - ons, user IDs, to prevent unauthorized access

- verification and authentication of transactions or procedures to prevent and to minimize damage affecting data integrity

- periodic comparison of file content of electronic protected health information

6. The Security Officer is responsible to document authentication actions, accountabilities, recording results and reporting discrepancies.

7. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Technical Safeguards for Authentication of Persons and Entities

Reference: 45 CFR 164.312 (Required)

POLICY: It is the policy of the Plan to implement technical safeguards for authentication of persons and entities seeking access to electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to implement technical safeguards for authentication of persons and entities seeking access to electronic protected health information.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems and to identify methods and procedures for authentication of persons and entities seeking access to electronic protected health information.

3. The Security Officer may meet with other personnel to identify individuals and entities authorized to gain access to protected health information held by the Plan.

4. The Security Officer may confer with the management of health care providers, health care clearing houses, government agencies, business associates and others to establish electronic data interchange procedures, systems, protocols, and methods of authentication of persons or entities seeking access to electronic protected health information held by the Plan.

5. Examples of methods and procedures for authentication of electronic protected health information may include:

- periodic inspection and testing of system software authentication components

- verification and authentication of access transactions or procedures to prevent unauthorized access

- verification, authentication matching of passwords, log-ons, or other automated "system handshakes" to prevent unauthorized access

- verification and authentication of transactions or procedures to prevent alteration or destruction of electronic protected health information.

- periodic comparison of file content of electronic protected health information

6. The Security Officer is responsible to document authentication actions, accountabilities, recording results and reporting discrepancies.

7. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Technical Safeguards to Protect Data Transmission Security

Reference: 45 CFR 164.312 (Addressable)

POLICY: It is the policy of the Plan to implement technical safeguards to protect data transmission security of electronic protected health information.

PROCEDURE:

1. The Security Officer is responsible to implement technical safeguards to protect data transmission security of electronic protected health information. Data transmission security safeguards may focus on audit of system hardware, software, or procedural mechanisms.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems that transmit electronic health information and to develop data transmission procedures that reasonably and appropriately safeguard data.

3. The Security Officer may confer with the management of health care providers, health care clearing houses, government agencies, business associates and others to establish transmission security procedures as part of electronic data interchange procedures, systems, and protocols assure protected transmission of protected health information to or from by the Plan.

4. Examples of a system hardware transmission safeguards may include:

   - Periodic inspection and testing of system hardware components handling transmissions,

   - Installation of transmission security devices to prevent alteration or destruction or disclosure of information during the transmission process,

   - Installation of locking devices or systems to prevent unauthorized access to transmission systems to prevent unauthorized physical access to such equipment,

   - Installation of "firewall" or similar electro-mechanical systems designed to block and/or detect unauthorized access or damage by malicious software,

   - Evaluation and specification of hardware components to assure compatibility preventing unauthorized access affecting data integrity during transmission process.

5. Examples of a transmission security system software integrity safeguards may include:

   - Periodic inspection and testing of system software components,

- Implementation if integrity controls to ensure that electronically protected health information is not improperly modified without detection until disposed of,

- Installation of encryption and decryption mechanisms designed to block and/or detect unauthorized access or damage by malicious software or unauthorized personnel.

6. The Security Officer is responsible to document technical safeguards to protect data transmission security through definition of written procedures defining procedural steps, accountabilities, recording results and reporting discrepancies.

7. The Security Officer is responsible to re-evaluate these issues and plans on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan.

Policies, Procedures and Documentation

Reference: 45 CFR 164.316 (Required)

POLICY: It is the policy of the Plan to develop policies, procedures and documentation to demonstrate compliance efforts with HIPAA security requirements.

PROCEDURE:

1. The Security Officer is responsible to develop policies, procedures and documentation to demonstrate compliance efforts with HIPAA security requirements.

2. The Security Officer is responsible to evaluate the Plan's electronic information systems that transmit electronic health information and to develop reasonable and appropriate policies, procedures and documentation.

3. The Security Officer may confer with other Employer staff personnel to establish security or related procedures and documentation to establish controls to protect health information and demonstrate compliance with the HIPAA security regulation.

4. Examples of policies and procedure to comply with the General Rules of the HIPAA security standard include:

- Implementing reasonable policies and procedures to comply with the standards, implementation specifications, and other requirements of the regulation.

- Implementation of policies and procedures in written or electronic form,

- Implementation of a written record (in written or electronic form) where required the HIPAA security regulation

5. The Security Officer is responsible to retain documentation for 6 years from the date of its creation or the date when it last was in effect, which ever is longer.

6. The Security Officer is responsible to make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

7. The Security Officer is responsible to re-evaluate policies and procedures on an annual basis, considering changes in Plan operations, changes in technology or equipment, changes to applicable regulations, and other factors that may affect the security of electronic protected health information held by the Plan and to update policies and procedures as needed.

Disciplinary Procedures (Sanction Policy)

Reference: 45 CFR 164.308 (Required)

POLICY: It is the policy of the Plan to communicate information to Plan and the Employer's employees, officers, and agents about standards of conduct and to use corrective disciplinary action when needed to address policy violations, correct employee misconduct and improve job performance.

PROCEDURE:

1. The Security Officer is responsible for communicating policies and standards of conduct to subordinates and others. At time of affiliation with the Employer, each individual shall receive appropriate orientation documents.

2. Each individual is responsible to perform assigned duties in a safe, professional, and efficient manner while conducting himself or herself in a manner which observes practice privacy and security policies.

3. The Security Officer is responsible to enforce compliance with policies and deal with misconduct according to the guidelines of this policy. In the event of violation of Plan privacy or security policies, appropriate corrective disciplinary action shall be taken. Corrective action may be in the form of coaching, discussion, re-training, a verbal warning, a written warning, suspension without pay, or dismissal.

4. When conducting a disciplinary discussion with an individual, it is recommended that:

    a) the discussion be conducted in a private office or other similar area;

    b) the individual be told what actions constituted misconduct and what form of corrective or disciplinary action is being taken;

    c) an individual may request that another representative be present if a discussion will result in disciplinary action.

5. All disciplinary actions (including verbal warnings) are to be documented on the Employee Counseling Sheet which is attached. The counseling sheet should be signed by the individual and the appropriate Employer officer or Security Officer. If the individual refuses to sign, another Manager/witness shall note on the form that the individual refused to sign. One copy of the form shall be routed to the individual's personal file; and the individual may receive a copy.

FORMS

Security Officer Job Description

Summary: The Security Officer is responsible for developing and implementing policies, procedures and safeguards to protect the privacy of health information and to assure compliance with The HIPAA Security Rule. May perform other specified tasks and responsibilities.

Essential Duties & Responsibilities:

- Plans, develops and implements security policies and procedures.

- Serves as contact person responsible for receiving incident reports related to security of protected health information.

- Plans and conducts or coordinates training for the Employer's staff regarding the Security Rule, Plan policies and procedures related to security of protected health information.

- Schedules training to implement security rule procedures, training for new hires or newly affiliated individuals and training when functions are affected by a material change in policies and procedures.

- Documents training content and individual participation in training.

- Evaluates administrative, technical and physical practices or conditions to assure security of protected health information and implements safeguards to protect against unauthorized use or disclosure of such information.

- Develops, implements and maintains a process to document and resolve security incidents.

- Develops and communicates sanctions against individuals who fail to comply with security policies and procedures.

- Enforces or recommends enforcement actions action against individuals for policy violations, and documents sanctions applied.

- Recommends and implements any corrective action as feasible to mitigate any harmful effect of unauthorized use or disclosures of protected health information.

- Monitors implementation of security policies and procedures to prevent and guard against any retaliation towards individuals for exercise of rights under the security rule.

- May retain and direct work activities of independent professionals such as systems or programming or security professionals to handle administrative, physical or technical aspects of the Employer's security plan.

- Monitors changes to security rule requirements and implements changes to policies and procedures as needed, documenting such changes and providing individual training.

- Maintains and supervises maintenance of files, records and documents created to comply with the security rule.

- Performs tasks in office or healthcare facility area. Moves and handles documents and other light weight items. Tasks requires moderate to frequent handling/use of office equipment. Performs other duties as assigned.

Job duties are subject to change as directed by management.

Assessing Addressable Implementation Standards

Instructions: The HIPAA security regulation defines certain "required" implementation standards which must be implemented and certain "addressable" standards which should be implemented if reasonable and appropriate. Use this form to document Employer's process of assessing "addressable" implementation standards. [Reference: 164.306 (b)(3)(ii)] (See sample policies for identification of addressable standards)

Implementation Standard #_____ Implementation Standard Topic_____

Summary of content of "addressable" Implementation Standard

_____

_____

Does the Implementation Standard deal with an issue that affects the Plan, its computer system, facility, or its electronic protected health information?

Yes No

Is there an actual or potential threat or likelihood of such event affecting the Plan, its computer system, facility, or its electronic protected health information?

Yes No

Is the Implementation Standard reasonable and appropriate for the Plan, its computer system, facility, or its electronic protected health information?

Yes No

If the implementation standard is not reasonable and appropriate, identify why and attach any relevant documentation.

_____

If the implementation standard is not reasonable and appropriate, identify any alternative measure that is reasonable and appropriate.

_____

Assessment performed by:

_____ _____ _____

Name & Signature Title Date

Risk Analysis

Instructions: The HIPAA security regulation requires covered entities to conduct a risk analysis. The risk analysis should be an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, integrity and availability of electronic PHI held by Employer. This form guides and documents the risk analysis [Reference: 164.308 (a)(1)(ii)(A)]

Potential Threat	**Estimated Level of Risk**	**Comment**
Unauthorized system access	High Medium Low	_____
Unauthorized clearance to system	High Medium Low	_____
Access by Terminated user	High Medium Low	_____
Unauthorized system access	High Medium Low	_____
Failure to isolate PHI within entity	High Medium Low	_____
Failure to respond to access changes	High Medium Low	_____
Inadequate training for users	High Medium Low	_____
Failure to verify access authorization	High Medium Low	_____
Failure to respond to security incidents	High Medium Low	_____
Loss or alteration of data	High Medium Low	_____
Failure to anticipate security contingencies	High Medium Low	_____
Unauthorized disclosure by Business Associate	High Medium Low	_____
Security penetration due to inadequate facility access controls	High Medium Low	_____
Failure to instruct users on workstation use	High Medium Low	_____

Disclosure from inadequate workstation security	High	Medium	Low	_____
Disclosure from to inadequate device and media controls	High	Medium	Low	_____
Loss of data integrity	High	Medium	Low	_____
Receipt of unauthenticated data	High	Medium	Low	_____
System access by unauthenticated persons or entities	High	Medium	Low	_____
Loss or disclosure of data during transmission	High	Medium	Low	_____
Liability due to inadequate documentation of security practices	High	Medium	Low	_____
Other:_____	High	Medium	Low	_____
Other: _____	High	Medium	Low	_____

Definitions for estimated level of risk:

High - There is a high level or significant likelihood that the anticipated risk may occur.
Medium - The likelihood of a risk occurring is judged to be of a moderate or medium level of risk.
Low - The likelihood of a risk occurring is judged to be minimal or unlikely.

Risk Management Worksheet

Instructions: The HIPAA security regulation requires covered entities to conduct a risk analysis and then to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. This form is designed to guide the risk management process. Be sure to implement an appropriate administrative or physical or technical safeguard for each risk identified. [Reference: 164.308 (a)(1)(ii)(B)]

Potential Threat	**Specify security measure implemented**	**Date Completed**
Unauthorized system access		
Unauthorized clearance to system		
Access by Terminated user		
Unauthorized system access		
Failure to isolate PHI within entity		
Failure to respond to access changes		
Inadequate training for users		
Failure to verify access authorization		
Failure to respond to security incidents		
Loss or alteration of data		
Failure to anticipate security contingencies		
Unauthorized disclosure by Business Associate		
Security penetration due to inadequate facility access controls		
Failure to instruct users on workstation use		

Risk Management (continued)

Disclosure from inadequate workstation security	_____	_____
Disclosure from to inadequate device and media controls	_____	_____
Loss of data integrity	_____	_____
Receipt of unauthenticated data	_____	_____
System access by unauthenticated persons or entities	_____	_____
Loss or disclosure of data during transmission	_____	_____
Liability due to inadequate documentation of security practices	_____	_____
Other:_____	_____	_____
Other:_____	_____	_____

Information System Activity Review

Instructions: The HIPAA security regulation requires covered entities to regularly review records of information system activity, such as audit logs, access reports, and security incident reports. This form is designed to guide and document the information system activity review process. [Reference: 164.308 (a)(1)(ii)(D)]

System Activity	Record/Report Reviewed	Date	Comment
Audit Logs	Audit Log Report	_____	_____
User Access	Access Report	_____	_____
Security Incidents	Incident Report	_____	_____
User changes/terminations	Access Report	_____	_____
User Training	Training Acknowledgments	_____	_____
Other	_____	_____	_____
Other	_____	_____	_____
Other	_____	_____	_____
Other	_____	_____	_____

Request for Authorization to Access PHI

(Protected Health Information) Based on Work Function

The Employer permits only authorized individuals to gain access to and work with protected health information. This form documents the request for authorization for eligible individuals based on work function. Submit this form to the Security Officer for approval.

Individual Name_____ Date of Request_____

Access is: _____ New _____ Changed

Period of access
_____Indefinite
_____ For a specified duration, beginning date_____to ending date_____

Work Function justifying access to PHI

Job_____ Reason for Access_____

Workstation assignment_____
_____ PHI Eligible workstation
_____ non-eligible workstation

Work Transaction(s) performed (attach job description)
_____ Maintenance of Patient record
_____ Coding for billing
_____ Insurance Claim Processing
_____ Medicare Claim Processing
_____ Other Claim processing
_____ Other_____

Program/Process operated
_____ Patient Record
_____ Billing
_____ Coding
_____ Conversion
_____ Other_____

Clearance level (Check appropriate level)
_____Level 0 _____Level I _____Level II
_____Level III _____Level IV _____Level V _____ Level VI

Comment:_____

Individual:_____ Supervisor:_____

Clearance and Authorization to Access PHI

(Protected Health Information)

The Employer permits only authorized individuals to gain access to and work with protected health information. This form documents Clearance and Authorization for eligible individuals.

Individual Name_____ Date of Request_____

Job_____ Purpose of Access_____

Period of access:

_____Indefinite

_____Of specified duration, beginning date_____to ending date_____

Clearance level (Check appropriate level)

Access Level	**Definition**
_____Level 0	Not eligible for access
_____Level I	Able to view selected screens or data based on job function. May print data to pre-defined reports.
_____ Level II	Able to view selected screens, enter data and print reports based on job function.
_____Level III	Able to view selected screens, enter data change or correct data, sort data and print reports based on supervisory role for job function.
_____Level IV	Authorized access to multiple data base sectors based on management role Able to view selected screens, enter data change or correct data, sort data and print reports
_____Level V	Authorized access to all system data base sectors based on management role Able to view selected screens, enter data change or correct data, sort data and print reports
_____Level VI	Authorized access to programs, code and system controls to design and maintain system.

Access is _____ Authorized _____ Denied

Reason:_____

Comment:_____

_____ _____

Security Officer Date

Record of Employees Authorized to Access PHI

(Protected Health Information)

Instructions: This form provides a record of individuals who are authorized for access to protected health information, documenting date and reason for authorization, change and ultimately, termination. This record will be maintained be the Security Officer.

Key: Authorization action 1. Granted; 2. Denied; 3. Changed; 4. Terminated

Individual Authorization Date	ID #	Job	Function or Reason	Action

Termination of Authorization to Access PHI

(Protected Health Information)

The Employer permits only authorized individuals to gain access to and work with protected health information. This form documents the termination of Authorization for individuals no longer eligible to access electronic protected health information.

Individual Name_____ Job_____

Reason for Termination of Access_____

Period of Termination of Access

_____ Indefinite
_____ Of Specified duration, beginning date_____to ending date_____
_____

Clearance level prior to termination

_____Level I _____Level II _____Level III
_____Level IV _____Level V _____Level VI

Access is Terminated effective Date & Time:_____

Follow-up action

_____a) Document new affiliation status of individual
_____b) System adjustment to block use of individual's password and log-in code.
_____c) Periodic revision of password and log-on codes
_____d) Re-assignment of tasks performed by individual now terminated from access.
_____e) Notification of affected individuals, departments or outside organizations relating to re- assignment of responsibilities.

Comment:_____

_____ _____ _____
Supervisor Security Officer Date

Training Announcement

Memorandum

To: All Individuals Performing Services for the Illinois Educators Risk Management Program Group Health Plan
From: Lori Eisenmenger, Plan Security Officer
Date:
Subject: New Privacy Security Policies

We are all familiar with the government rules concerning the privacy of health information under the Health Insurance Portability and Accountability Act of 1996, known as HIPAA. The regulations also require that covered entities take certain precautions to protect the security of electronic protected health information. This portion of HIPAA is referred to as the Security Rule.

The HIPAA Security Rule requires health care providers to implement certain security safeguards addressing administrative, physical and technical protections relating to use and disclosure of electronic health information. To comply with the regulations, the Illinois Educators Risk Management Program Association is implementing the following actions:

1. Lori Eisenmenger has been appointed as Security Officer for the Plan.

2. The Plan board has created policies and procedures to guide Plan personnel in proper handling and use of electronic protected health information as required by the Security Rule.

3. All Plan personnel are scheduled for security training beginning in the near future. You will be notified of your scheduled training date and time.

4. Details of these new security policies are defined in a written security policy manual which is maintained by the Security Officer. Individuals in certain positions will received detailed instructions and procedures for implementing these new policies. The security policies are effective immediately.

Training Acknowledgment

Training Acknowledgment

I hereby acknowledge that I have participated in HIPAA Security Standards training and have been advised of the Illinois Educators Risk Management Program Group Health Plan's security policies and procedures, including information on the topics listed below:

Overview of HIPAA Medical Privacy Requirements

HIPAA Security Standards - General Rules (164.306)

Administrative Safeguards (164.308)
Including assigned responsibility, security management process, workforce security, information access management, security awareness & training, security incident procedures contingency plan, evaluation of contingency plan, and business associate contracts

Physical Safeguards (164.310)
Including facility access controls, workstation use, workstation security, device and media controls.

Technical Safeguards (164.312)
Including access control procedures, audit controls integrity protecting information, person or entity authentication and transmission security

Organizational Requirements (164.314)
Including business associate contracts and group health plans

Policies Procedures and Documentation (164.316)
Including overview of the Plan’s policies and procedures and documentation

Compliance Dates (164.318)

Individual's Name	**Signature**	**Date**

Security Reminders

(#1)

Protect Your Password

Remember. . .

. . . Protect the privacy and security of the protected health information at your workstation.

. . . Do not share or divulge your system password to others.

. . . Report any unusual activity or security incidents to your Supervisor

(#2)

Protecting Privacy and Security
It's everyone's job

. . . Do not share or divulge your system password to others.

. . . Be sure to observe proper operating procedures to protect the security of the information.

. . . Report any unusual activity or security incidents to your Supervisor

Audit Report for Verification of Access Authorization

This report provides a format for an audit report showing system verification of access authorization comparing individual transactions to the employee's assigned password and log on codes.

Transaction Number	Date/Time	Transaction Password	Transaction Log-on	Individual Password	Individual Log-on	Compare to Individual Discrepancy? Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No
_______	_______	_______	_______	_______	_______	Yes	No

_____ _____ _____ _____ _____ _____

Yes No

Action by Security Officer in the event of Discrepancy:

_____

_____

Establishment Authorization to Access PHI

(Protected Health Information)

The Illinois Educators Risk Management Program Group Health Plan permits only authorized covered entities and/or business associates to gain access to and work with protected health information created or held by the Health Care Plan. This form documents Authorization for eligible establishments to gain such access.

Entity

Establishment Name_____Date of Request_____
Address:_____City:_____ State:_____ ZIP_____

Phone:_____ Fax:_____
Contact:(1)_____ E-mail_____
(2)_____ E-mail_____

Purpose justifying access to PHI

_____ Covered Entity _____Business Associate _____Other

Reason for Access_____

Work Transaction(s) performed

_____Referral for health care services
_____Referral for prescribed products or services
_____Referral for lab/analytical services
_____Maintenance of Patient record
_____Coding for billing
_____Insurance Claim Processing
_____Medicare Claim Processing
_____Other Claim processing
_____Conversion to Standard formats
_____Conversion from Standard Formats
_____Other_____

Access is: _____ New _____ Changed _____ Terminated
Reason::_____

Period of access
_____Indefinite
_____ For a specified duration, beginning date_____to ending date_____

Comment:_____

_____
Security Officer

Security Incident Report

The HIPAA Security regulations define certain security precautions intended to guide proper handling of protected health information. If you have observed an unusual incident or event or believe that the security of protected health information held by the Plan may have been compromised, you have a responsibility to report the incident, using this Security Incident Report form. Please complete this security incident report form to provide details to so that we may investigate and attempt to resolve the matter.

Name:_____ Work station I.D. _____

Job:_____

Date of incident:_____ Time of incident:_____

Describe incident:_____

_____

_____

_____

_____

Return this form to: the Plan's Security Officer.

This section to be completed the Plan's Security Personnel

Security Officer's investigation:_____

_____

_____

_____

_____

Follow-up action:_____

_____

_____

_____

_____

_____ _____

Security Officer Date

.

Security Incident Response and Report

Memorandum

To: _____
Board President

From: _____
Security Officer

Re: Report of Security Incident
Occurring (date) _____

This office became aware of a security incident based upon receipt of a security incident report as identified above. This matter has been investigated resulting in a finding as summarized below:

_____The incident was investigated and found not to be a threat to the security of protected health information held by the Group Health Plan.

_____The incident was investigated and found to be a potential or actual threat to the security of protected health information held by the Group Health Plan.

Summary of finding: _____

_____

As a result of this finding, the following action is being taken:

_____A new administrative policy and procedure has been defined to correct the incident

_____A new technical process or procedure has been defined to correct the incident

_____A new physical process or facility modification has been implemented to correct the incident

_____A new piece of equipment or system feature has been installed to correct the incident

_____The affected individuals have received training relating to the new system, process or procedure.

_____The business associate identified below has been instructed to (start)(stop) making the requested use or disclosure. Business Associate_____

_____Other: (describe)_____

_____This matter will be subject to review an evaluation after the following time period:

Additional corrective action may be taken at that time as appropriate.

Worksheet for Evaluation of Data Security Contingency Plan

Organization:_____ Date of Evaluation:_____

1. Describe any security incidents occurring during the period of evaluation.
(Attach copies of Security Incident Reports.)

_____

2. Describe any Privacy Complaints occurring during the period of evaluation.
(Attached copies of the complaints.)

_____

3. Describe any unauthorized disclosure of protected health information occurring during the period of evaluation. (Attach copy of any relevant record or documentation of the disclosure)

_____

4. Describe corrective action taken for any incidents recorded in items #1, 2, or 3 above.

_____

5. Describe any facility changes occurring during the reporting period.

_____

6. Describe any equipment or systems or software changes occurring during the period of evaluation.

_____

7. Have there been any personnel or organizational changes occurring during the period of evaluation?

Describe:_____

8. Have there been any changes to the HIPAA Privacy or Security regulations? Yes No

If yes, describe:_____

9. Based on information in items # 1 through #8, is there a need to update the data security contingency plan? Yes No

If Yes, describe: _____
Identify below the portions of the plan to be updated:

Plan Elements	Result		Comment
	Current	Update	
Introduction	_____	_____	_____
Responsibility	_____	_____	_____
Impact Analysis	_____	_____	_____
Protecting Human Safety	_____	_____	_____
Notification Procedure	_____	_____	_____
Data Backup	_____	_____	_____
Disaster Recovery Plan	_____	_____	_____
Emergency Mode Operations	_____	_____	_____
Restoration and Recovery	_____	_____	_____
Testing and Revision	_____	_____	_____
Criticality Analysis	_____	_____	_____
Documentation	_____	_____	_____
Other:_____	_____	_____	_____

Facility Security Plan

Illinois Educators Risk Management Program
Group Health Plan
Facility Security Plan

Illinois Educators Risk Management Program Group Health Plan establishes the following facility security plan to protect individuals, data, and assets.

Responsibility

The Security Officer is responsible to manage the facility security plan. The plan shall consist of facility access control 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.

Alarm System

The plan administrator's facility is protected by a security alarm system. The alarm system monitors facility entrances, doorways, and windows for unauthorized entrance during non-business hours. The alarm system is activated at the end of the work day by the Security Officer and de-activated by a designated individual responsible to open the facility.

The Security Officer is responsible to coordinate with the system vendor to maintain the security system, and to control system access codes permitting activation and de-activation. The codes shall be changed at periodic intervals as directed by the Security Officer and/or as specified by the system vendor. Arrangements shall be made for access by the building owner and by janitorial services personnel. Such arrangements shall specify the need to protect the security of the Health Care Plan electronic protected health information, equipment, and records.

Key Control

The plan administrator's facility is protected by locked entrances. The key and lock system secures facility entrances and doorways from unauthorized entrance during non-business hours. All doorways are to be locked at the end of the work day by the last individual leaving the facility.

Designated supervisors and employees receive keys. The Security Officer is responsible to issue keys, record issuance of each key, and provide guidelines relating to use of keys. Keys may not be duplicated. Keys shall be returned upon separation of employment. In the event of loss of a key, re-keying of locks shall be ordered.

The Security Officer is responsible to coordinate with the building owner to maintain the security facility locks. Arrangements shall be made for access by the building owner and by janitorial services personnel. Such arrangements shall specify the need to protect the security of the Health Care Plan electronic protected health information, equipment, and records.

Communications and Power Systems

Communications systems and power trunk lines shall be centered into a locked communications closet. Key control procedures shall be implemented as defined above. Key access shall be limited to the Security Officer and one backup individual. All access to the communications closet and any work on communications or power lines shall only occur upon the order or authorization of the Security Officer and coordinated with the building owner as necessary.

Back-up power systems shall be procured and maintained as deemed necessary by the Security Officer.

Central computer network servers shall be stored in a locked systems closet. Individual computer terminals shall be evaluated and secured by one or more of the following:

- CPU cabinet locking device
- Keyboard locking device
- Bolting of terminal to furniture, fixture, or wall
- Bundling, strapping or hiding of wiring connections.

Visitors

All visitors shall enter through the reception area and wait in the reception area until called by an appropriate employee.

- Vendors shall be verified for purpose of visit and escorted to area or office or individual relating to the purpose of their visit.
- Solicitors shall be verified for purpose of visit and escorted to area or office or individual relating to the purpose of their visit.

Records

The Security Officer is responsible to maintain record documenting physical security protections and activity. Records shall include:

Inventory listing of equipment
Assignment of equipment to specified individuals, as appropriate,
Check out/check-in documentation of portable equipment
Key control record
Security control instructions & record
Equipment maintenance or service record
Authorized service vendors
Service vendor agreements or other similar records.

Individual Warning Notice

Name _____ Date _____

Department _____

You are hereby notified that, if you repeat the offense described below or permit the condition described to continue to be repeated, your employment relationship with this company may be terminated without further notice.

Offense: _____

_____

Management Action:

____ Verbal Warning ____ Written Warning

____ Suspension _____ ____ Termination
(From/to)

_____ _____ _____ _____
Individual Date Officer Date

Emergency Contingency Plan

Illinois Educators Risk Management Program
Group Health Plan
Emergency Contingency Plan

Introduction

Illinois Educators Risk Management Program Group Health Plan has established this contingency plan to promote preparedness and timely response to emergency situations or incidents. This plan is designed to minimize the adverse affect of such incidents upon the organization, protect the safety of affiliated individuals and participants, permit continued operations with a minimum of disruption, protect the Health Care Plan assets and protected health information.

The Health Care Plan's contingency plan addresses anticipated potential minor incidents as well as major disasters. While it is recognized that not every conceivable disruption or disaster can be anticipated, it is expected that this contingency plan will serve as an outline to guide timely response.

Responsibility

The Plan Sponsor has recognized the need to assign responsibility for implementation of various aspects of the contingency plan. The assignment of responsibility promotes greater preparedness and timely response to emergency situations or incidents. Responsibility is assigned as shown below:

The Plan Sponsor's management bear ultimate responsibility for prudent management of the Health Care Plan including development and implementation of sound management practices to safeguard protected health information. Day to day accountabilities are assigned to specified individuals as described herein.

The Security Officer is responsible for planning, development and administration of the Health Care Plan Contingency Plan. This includes conducting an analysis of security threats and developing reasonable and appropriate response to such threats.

The Security Officer is responsible for maintaining records and documentation of the contingency plan and for training employees as necessary.

The Security Officer is responsible to direct affiliated individuals to carry out the contingency plan in a manner that assures service quality.

Business Emergency Impact Analysis

The business emergency impact analysis examines potential threats and their impact upon the organization. The analysis identifies the likelihood of such threats and specifies a response priority. This analysis is summarized below:

Threat category

Threats to	Threats to
Data and documents	Facilities and equipment

Examples of Threats

Minor Incidents

Temporary power loss	Minor accident causing
Penetration attempt	Facility or equipment damage

Major Incidents

Penetration of system	Penetration of facility
Alteration/destruction of data	Destruction of facility
Fire or explosion	Destruction of equipment
Weather/geological disaster	Fire or explosion
Major power loss	Weather/geological disaster
Communications disruption	Major power loss
Communications disruption	

Response priority

First	Second

Data Backup

The Data Backup Plan shall consist of the following elements:

1. The Security Administrator is responsible to set computer system controls to run daily backups at a fixed time.

2. _____is responsible to check the computer system as the first task in the morning to verify that a backup of all electronic health information has been prepared.

3. _____ is responsible to follow established procedure to allow a full system backup at the end of each week, to be scheduled over the weekend.

4. Backup media shall be stored off-site at a secure location designated by the Security Officer. The off-site location is:_____.

5. _____ shall maintain a log of backup activities.

6. In the event of a system emergency, the Security Officer or his designee shall obtain the backup media to restore the system.

7. Backups shall include the operating system, applications, and data.

Disaster Recovery Plan

The Disaster Recovery Plan shall consist of the following elements:

1. A disaster recovery location will be designated by the Security Officer.

Emergency Contingency Plan

1. Backup media (including the operating system, applications, and data) shall be maintained at a separate off-site location as designated by the Security Officer.

2. In the event of a stem emergency, the Security Officer or his designee shall obtain the backup media to restore the system.

Emergency Mode Operations

The Emergency Mode Operation Plan shall consist of the following elements:

1. Staff shall provide regular Group Health Plan services to the extent possible based on availability of suitable facilities, equipment and personnel.

2. Facilities and/or equipment shall be restored as quickly as possible.

Restoration and Recovery

The Security Officer is responsible to establish and implement procedures that allow facility access in order to begin restoration and recovery.

1. In the event that access has been denied due to public safety or law enforcement investigative actions, the Security Officer shall meet with appropriate officials to negotiate access for recovery & restoration.

2. In instances where outside professionals are contracted for recovery or restoration activities, such entities shall be considered to be business associates, subject to a business associate agreement.

3. The Security Officer shall make arrangements allowing access for restoration while observing reasonable controls to protect the security of the Group Health Plan's assets and data.

Emergency Contingency Plan

Testing and Revision Procedures

The Security Officer is responsible to develop and implement any procedures as necessary for testing and revision of data security contingency plans. Revisions may occur as a result of new equipment, technologies, office relocations, personnel changes or experiences in implementing the contingency plan. The Security Officer shall confer with others as needed to test and revise policies and procedures to accomplish this objective.

Criticality Analysis

The Security Official is responsible to develop and implement any procedures as necessary to assess the relative criticality of specific applications and data in support of the contingency plan components. The following contingencies shall be made:

1. Arrangements shall be made with a system vendor for restoration of application software damaged or destroyed during an emergency incident.

2. The backup media shall be maintained at a separate off-site location as designated by the Security Officer, for re-installation as needed.

3. The Security Officer shall evaluate and select as the disaster recovery system a loaned computer, temporary loaned system access from another medical provider, rental, or leased system hardware. Such arrangement shall be re-evaluated not less than annually and revised as necessary to assure effective contingency operations.

Documentation

The Security Officer is responsible to maintain the contingency plan, to review the plan annually and to update the plan as needed. Copies of the plan shall be held by the Security Officer.

Effective: Date_____

Copies given to: _____ Date: _____

_____ Date: _____

_____ Date: _____

Emergency Contingency Plan

Record of Revisions:

Date	Topic	Comment

Checklist to Evaluate Facility Security Plan

Audit Schedule __Weekly, __ Monthly, __ Quarterly, __ Annually

Conducted by:_____ Date:_____

Areas of Audit	Result	Corrective Action Needed?
Responsibility		
Is security responsibility clearly defined?	_____	_____
In department	_____	_____
Overall	_____	_____
Has employee responsibility been defined?	_____	_____
Have job descriptions been updated to reflect current responsibilities?	_____	_____
Have employees been trained?	_____	_____
Alarm System		
Does the facility have an alarm system?	_____	_____
Does the department have an alarm system?	_____	_____
Are activation-deactivation procedures defined?	_____	_____
Is responsibility assigned for activation -deactivation?	_____	_____
Is alarm system tested?	_____	_____
Date-result of last test	_____	_____
Surveillance system tested?	_____	_____
Key Control		
Does facility have locked		
__ Building entrance	_____	_____
__ Office entrance	_____	_____
__ Employee -service entrance	_____	_____
__ Windows,	_____	_____
__ Records storage	_____	_____
__ Controlled Substance storage	_____	_____
__ other_____	_____	_____
Who is responsible for key control?	_____	_____
Criteria for issuing of keys:	_____	_____
List of employees receiving keys	_____	_____
Procedure for lost keys	_____	_____
Procedure for return of keys	_____	_____
Communications and Power Systems		
Security or lock status of		
__ Communications systems	_____	_____

__ power trunk lines _____ _____
__Circuit breaker control _____ _____

Checklist to evaluate your Facility Security Plan

__ Emergency or back-up power _____ _____
__telecommunication network _____ _____
__ Other:_____ _____ _____
Access procedure defined _____ _____
Responsibility defined _____ _____
Maintenance access procedure defined _____ _____

Central Computer Network
Security or lock status of
__ Communications systems _____ _____
__ Power trunk lines _____ _____
__ Circuit breaker control _____ _____
__ Emergency or back-up power _____ _____
__ Telecommunication network _____ _____
__ Other:_____ _____ _____

Access procedure defined _____ _____
Responsibility defined _____ _____
Maintenance access procedure defined _____ _____
Personal computer terminals _____ _____
- CPU cabinet locking device _____ _____
- Keyboard locking device _____ _____
- Bolting of terminal to furniture, fixture, or wall _____ _____
- Bundling, strapping or hiding of wiring connections. _____ _____
- View Screens –Screensaver _____ _____
- password controls _____ _____

Visitors Procedure defined
Patients _____ _____
Vendors _____ _____
Solicitors _____ _____
Maintenance-services _____ _____

Records
Status of records documenting physical security protections and activity.
__ Inventory listing of equipment _____ _____
__ Assign equipment to specified individuals, as appropriate _____ _____
__ Check out/check-in documentation of portable equipment _____ _____

__ Key control record	_____	_____
__ Security control instructions & record	_____	_____
__ Equipment maintenance or service record	_____	_____
__ Authorized service vendors	_____	_____
__ Service vendor agreements	_____	_____
__ other similar records _____	_____	_____

TRAINING MATERIALS

Training Leaders Guide

Overview

Organizations subject to the Health Insurance Portability and Accountability Act of 1996 are required to adopt new privacy and security protections. This Act is often referred to as HIPAA.

HIPAA creates national standards to protect an individual's medical records and other health information created or maintained by the Health Care Plan. The HIPAA Privacy Rule, which had a compliance date of April 14, 2003, required covered organizations to develop policies designed to protect privacy of health information and to guard against unauthorized disclosures in the administration of policies.

The HIPAA Security Rule requires covered organizations to develop administrative, physical and technical safeguards to protect health information. The HIPAA Security Standards appear in the Code of Federal Regulations at 45 CFR Parts 164.308 through 164.318.

Compliance Schedule

The HIPAA Security Rule has a compliance date of April 20, 2005. By that date, covered entities must have in place administrative controls such as policies, procedures and documentation to demonstrate efforts taken to provide physical and technical safeguards for protected health information created and maintained by the entity.

Covered Entities

The HIPAA Security Rule applies to the same entities covered by the HIPAA Privacy Rule. This includes health plans, health care clearing houses, and those healthcare providers who conduct certain financial and administrative transactions (e.g. electronic billing, and funds transfers) electronically. The provisions apply equally to organizations in the private and the public sectors.

Administrative Safeguards

The HIPAA Security Rule requires covered entities (i.e., the Group Health Plan) to develop certain administrative safeguards. Examples of administrative safeguards include: assigning security responsibility, developing a security management process, creating guidelines for workforce security, specifying procedures for information access management, providing security awareness and training, defining security incident procedures, creating and evaluating a Contingency Plan.

Physical Safeguards

The HIPAA Security Rule requires that organizations develop and implement physical safeguards which protect the facility and equipment used by the covered entity. This aspect of the security plan should address facility access controls, provide procedures on workstation use, define guidelines for workstation security, and specify requirements for device and media controls.

Technical Safeguards

The HIPAA Security Rule requires that organizations develop and implement technical safeguards which protect data and define controls to limit who has access to protected health information. Such safeguards may include access control procedures, audit controls, protecting integrity of information, authentication of persons or entities accessing information and provisions for protecting transmission security.

Organizational Requirements

The HIPAA Security Rule requires that covered entities define procedure safeguards relating to the handling or use of protected health information by Business Associates and group health plans.

Policies Procedures and Documentation

The HIPAA Security Rule requires that covered entities define and implement policies and procedures relating to security issues and to document actions taken to comply with the rule.

Required and Addressable Actions

According to the HIPAA Security Standard, certain **Required** actions must be implemented in the organizations security plan.

Additionally, certain **Addressable** actions may be assessed and implemented as reasonable and appropriate.

In the event that an addressable action is not implemented, such action shall be documented, identifying reason(s) for not taking such action and identifying other equivalent alternatives implemented.

Our Security Objectives

The Plan is committed to managing its information system in a manner which achieves the objectives listed below. It is our objective:

- to ensure the confidentiality, integrity and availability of all electronic protected health information which is created, received, maintained or transmitted in the course of providing health care services;

- to protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

- to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under Privacy Rule regulations;

- to ensure that employees perform tasks in compliance with HIPAA privacy and security standards.

Responsibility

The Plan has designated Lori Eisnemenger as the "Security Officer". This individual will be responsible for the development and implementation of the security management process.

The Security Officer is responsible to implement the following "Required" security management activities:

+ Conduct a Risk Analysis
+ Risk Management
+ Sanction Policy
+ Information System Activity Review

"Required" security management activities

a) Conduct a Risk Analysis. The risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of protected health information held by the Health Care Plan in electronic form.

b) Risk Management. Risk management is the development and implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

c) Sanction Policy. A sanction policy guides enforcement by defining sanctions or other corrective or disciplinary action which will be taken against violators.

d) Information System Activity Review. The information system activity review consists of procedural guidelines and actions for the periodic review of the organization's information system. A systems review includes review of systems records such as audit logs, access reports, and security incident tracking reports.

Access to Protected Health Information

The Security Officer is responsible to develop procedures for the control of access to electronic protected health information. Such access shall be based on job functions, responsibilities and system controls.

Access to protected health information by personnel is limited to the specific job related purpose of the work activity being performed. System design, password controls, system screen access are used to limited access to only those persons whose to job activities or functions require access to protected health information.

Your supervisor is responsible to identify individuals permitted to gain access, provide access instructions or procedures, and to supervise work activities to assure that access instructions are followed.

In the event that an individual changes jobs or if a job responsibilities change eliminating the defined justification for access to protected health information, action is taken to prevent further access by such individual to protected health information.

Levels of Access

Many computer systems holding protected health information define certain levels of access to the information. Depending on your job and responsibilities, your access to protected health information may be defined in a category as shown below:

Not eligible for access to protected health information.

Able to view selected screens or data based on job function. May print data to pre-defined reports.

Able to view selected screens, enter data and print reports based on job function.

Able to view selected screens, enter data change or correct data, sort data and print reports based on supervisory role for job function.

Training

The HIPAA Security Rule requires security awareness and training. The training covers the organization's security plan. Training is conducted:

- not later than the compliance date for the security rule.
- for all members of the workforce including management

In addition, as in the HIPAA Privacy Rule, training is recommended:

- for each employee whose functions or responsibilities change, resulting in access to protected health information;

- following any change in policies or procedures relating to HIPAA privacy or security requirements or changes to the HIPAA security rule or related regulations.

Security Audits and Checks

The Security Officer may establish a periodic audits and checks to verify a user's right to access and to assure compliance with security policies and procedures.
Examples of audits may include one or more of the following:

- Track of password(s) or other ID used to log onto protected health information system

- Track of password(s) or other ID used when entering transactions within the protected health information system

- Audit comparison of password or other ID corresponding to individual, workstation, or work activity

- Audit comparison of password or other ID corresponding to assigned clearance level, or work function

Security Incidents

The Security Officer will develop and implement security incident procedures. Security incidents are recorded on a security incident report form.

Individuals are reminded to be alert for common security incidents. Examples of security incidents may include one or more of the following:

- actual or attempted theft of records, data, or system equipment

- actual or attempted access to records, data, or system equipment by an individual who is not authorized for such access

- actual or attempted disclosure of records, data, or system security controls by an individual who is not authorized to make such disclosures or such disclosures are made to unauthorized persons.

- actual or attempted damage to or destruction of records, data, or system equipment.

- accidental disclosure or damage or destruction to records, data, or system equipment or other incident causing actual or attempted disclosure or damage or destruction of records, data, or system equipment.

In the event of any incident as described above, the employee shall immediately report the incident to his/her supervisor. The incident shall be documented on an Incident report.

The Security Officer will conduct an investigation into the incident.

Data Security Contingency Plan

The Security Officer will develop and implement a required data security contingency plan. The data security plan shall consist of the following "required" components and may contain certain addressable components:

- Data Backup Plan (required)
- Disaster Recovery Plan (required)
- Emergency Mode Operation Plan (required)
- Testing and revision procedures (addressable)
- Applications and data criticality analysis (addressable)

Data Backup and Recovery

The Data Backup Plan will consist of procedures to make backup copies of electronic protected health information and to store the backup copies at a designated separate location.

The Disaster Recovery Plan shall consist of the following elements:

- Back-up media (including the operating system, applications, and data) shall be maintained at a separate off-site location as designated by the Security Officer.
- In the event of a disaster incident, the following recovery plan shall be implemented as directed by the Security Officer and defined in the Emergency Mode Operation Plan.

The Emergency Mode Operation Plan shall consist of the following elements:

- Acquire necessary resources to perform a restore of computer system and medical applications.
- Back-up data shall be restored for use in providing services.
- Staff shall provide regular services to the extent possible based on availability of suitable facilities, equipment and personnel.

- Facilities and/or equipment shall be restored as quickly as possible.

Business Associates

The Plan will take action to ensure that any Business Associate shall be permitted to create, receive, maintain or transmit electronic protected health information on behalf of your organization is done only upon receipt of satisfactory assurances that the business associate will safeguard protected health information in accordance with requirements for the HIPAA security regulation.

Facility Access Controls

The Plan may establish facility access control 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.

Facility access controls may consist of one or more of the following action plans or control procedures.

- Contingency operations
- Facility Security Plan
- Access controls and validation procedures
- Maintenance Records

Examples of facility access control policies and procedures may include:

- Contingency operations -- Development of 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.
- Facility Security Plan -- Development of policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.
- Access controls and validation procedures -- Development of 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.
- Maintenance Records -- Development of policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (ie: computer hardware, walls, doors, locks, and power supply systems.

The foregoing list of facilities control action plans are considered addressable under HIPAA. The Security Officer will evaluate the need for such plan(s) and then implement plan(s) as needed to provide reasonable safeguards of electronic protected health information.

Guidelines on Workstation Use

The Plan will establish guidelines for workstation use to promote reasonable security and safeguards in the handling of electronic protected health information.

Set up and operation of a computer workstation must comply with the following guidelines:

- Only computer terminals, lap tops and peripheral equipment authorized by the Security Officer may be connected to the Plan's information system

- Only software or application programs authorized by the Employer may be installed or loaded onto the Employer's information system and /or terminals.

- Only designated individuals assigned to work functions relating to electronic protected health information may operate computer terminals, software or systems dedicated to handling such information.

- Computer terminals shall be secured to workstations in a manner prescribed by the Employer.

- Computer terminals in areas where individuals work multiple shifts shall be adapted with a locking device to prevent unauthorized access after regular working hours.

- Computer terminals shall be positioned to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals shall maintain a screen saver feature as authorized by the Security Officer to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals unavoidably positioned in an area where there are passers-by shall be fitted with a viewing filter as specified by the Security Officer to avoid or minimize likelihood of viewing of on-screen data by passers-by.

- Computer terminals used for entering or handling electronic protected health information shall be segregated into a special area, partitioned area or office to separate this activity from other non-HIPAA regulated information processing.

Privacy and Security Practices

Individuals performing authorized tasks involving use or disclosure of protected health information shall observe the following privacy and security practices:

- Do not share or disclose your password or log-on code with others.

- Do not access a secure data base in the presence of non-authorized persons.

- Do not leave your work area without first exiting the software application that handles protected health information.

- Be alert for any unusual incidents or unauthorized use or disclosure of protected health information and report such incident(s) to the Security Officer.

- Do not copy or download protected health information data except as authorized.

- Do not copy or download applications programs or software.

- Do not install other programs or software onto the employer's computer systems unless authorized.

Guidelines for Workstation Security

The Security Officer will establish guidelines for workstation security to promote reasonable safeguards for equipment and systems used in the handling of electronic protected health information. Set up and operation of a computer workstation must comply with the following guidelines:

- Only computer terminals, lap tops and peripheral equipment authorized by the employer may be connected to the employer's information system

- Computer terminals shall be secured to workstations in a manner prescribed by the Security Officer.

- Computer terminals in areas where individuals work multiple shifts shall be adapted with a locking devise to prevent unauthorized access after regular working hours.

- Access controls, such as locked or controlled access work areas shall be used to prevent access by unauthorized individuals and to verify proper access of individuals in the work area.

- Surveillance or other work area monitoring systems shall be used as deemed appropriated by the Security Officer.

Guidelines for Device and Media Systems

The Security Officer will responsible to establish guidelines to promote reasonable safeguards for device and media systems used in the handling of electronic protected health information. Set up and operation of a device and media systems must comply with the following guidelines:

- Only device and media systems authorized by the Security Officer may be connected to the Plan's information system.

- Device and media systems equipment shall be stored and secured in a manner prescribed by the Security Officer.

- Device and media systems in areas where individuals work multiple shifts shall be adapted with a locking device to prevent unauthorized access or use after regular working hours.

- Access controls, such as locked or controlled access work areas shall be used to prevent access to device and media systems by unauthorized individuals and to verify proper access of individuals working in the work area.

- Device and media systems may not be removed, altered, tampered with, or repaired except as authorized by the Security Officer.

- Device and media systems may not be reused or disposed of except as authorized by the Security Officer.

- Surveillance or other work area monitoring systems shall be used as deemed appropriate by the Security Officer.

Technical Safeguards for Access Control

The Security Officer will develop and implement technical policies and procedures for electronic information systems that maintain electronic health information to allow access only to those persons or software programs that have been granted access due to their responsibility and function.

The Security Officer will implement technical audit control policies and procedures for electronic information systems that maintain electronic health information to record and examine system activity. Control actions or procedures may focus on audit of system hardware, software, or procedural mechanisms.

The Security Officer will to implement technical safeguards to protect data integrity of electronic protected health information. Data integrity safeguards may focus on audit of system hardware, software, or procedural mechanisms.

The Security Officer will implement mechanisms to authenticate electronic protected health information. Such mechanisms shall corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. Data integrity mechanisms may include one or more of the following:

- Electronic file comparison

- Electronic file comparisons before and after transmission

- File size counts, tracking and comparison

- File access tracking and reporting

- Scheduled and random integrity checks.

The Security Officer will implement technical safeguards to protect data transmission security of electronic protected health information. Data transmission security safeguards may focus on audit of system hardware, software, or procedural mechanisms.

Documentation

The Security Officer will develop policies, procedures and documentation to demonstrate compliance efforts with HIPAA security requirements.

Examples of policies and procedure to comply with the General Rules of the HIPAA security standard include:

- Implementing reasonable policies and procedures to comply with the standards, implementation specifications, and other requirements of the regulation

- Implementation of policies and procedures in written or electronic form

- Implementation of a written record (in written or electronic form,) where required the HIPAA security regulation.

The Security Officer will retain documentation for 6 years from the date of its creation or the date when it last was in effect, which ever is longer.

Test Your Knowledge Quiz

The HIPAA Security Rule
Test Your Knowledge

Instructions: Read each question. Mark the correct answer by circling true or false.

Individual's Name:_____ Date:_____

The HIPAA Security Rule requires covered entities to develop administrative, physical and technical safeguards to protect the security of health information.	True	False
The HIPAA Security Rule applies to health plans, health care clearing houses and health care providers who conduct certain transactions electronically.	True	False
There is no requirement for a covered entity to assign responsibility to implement HIPAA security.	True	False
Certain required security management activities conducting a risk analysis, taking risk management actions to control risk, implementing a sanction policy, and conducting an information system activity review.	True	False
An addressable or recommended procedure is for a covered entity to define a procedure for granting access to protected health information which specifies eligible jobs and password controls.	True	False
There is no need to limit employee access to protected health information in an organization that has a healthcare clearinghouse function.	True	False
A covered entity is encouraged to define password procedures, monitor user log-in to the computer system, issue periodic security reminders and guard against malicious software.	True	False
A covered entity is required to create a Data Security Contingency Plan that includes a Data Backup Plan a Disaster Recovery Plan, and an Emergency Mode Operation Plan.	True	False
The HIPAA Security Rule requires a covered entity to develop a procedure for reporting and responding to security incidents.	True	False
An accidental disclosure or damage to electronic records due to a natural disaster such as fire for flood or not considered reportable security incidents.	True	False

A Business Associate's verbal promise or a "handshake deal" to protect security of health information is adequate assurance under the HIPAA Security Rule. True False

A covered entity is required to define workstation use and security procedures to safeguard against unauthorized access of protected health information. True False

The only requirement for disposal of obsolete media or devices is to place such items in the recycle bin. True False

A required technical safeguard is to establish a unique user identification (such as a password) for each individual who has access to protected health information. True False

Important rules for password use include: make your password a combination of alpha-numeric characters; do not share your password; do not use an alpha or numeric series (abc-123) in your password; and do not use an easily recognized identifier such as name, birthday or address. True False

Test Your Knowledge Answer Key

The HIPAA Security Rule
Test Your Knowledge- Answer Key

Note to the instructor: The correct response to each question appears in **bold.**

Individual's Name:_____ Date:_____

The HIPAA Security Rule requires covered entities to develop administrative, physical and technical safeguards to protect the security of health information. **True** False

The HIPAA Security Rule applies to health plans, health care clearing houses and health care providers who conduct certain transactions electronically. **True** False

There is no requirement for a covered entity to assign responsibility to implement HIPAA security. True **False**

Certain required security management activities conducting a risk analysis, taking risk management actions to control risk, implementing a sanction policy, and conducting an information system activity review. **True** False

An addressable or recommended procedure is for a covered entity to define a procedure for granting access to protected health information which specifies eligible jobs and password controls. **True** False

There is no need to limit employee access to protected health information in an organization that has a healthcare clearinghouse function. True **False**

A covered entity is encouraged to define password procedures, monitor user log-in to the computer system, issue periodic security reminders and guard against malicious software. **True** False

A covered entity is required to create a Data Security Contingency Plan that includes a Data Backup Plan a Disaster Recovery Plan, and an Emergency Mode Operation Plan. **True** False

The HIPAA Security Rule requires a covered entity to develop a procedure for reporting and responding to security incidents. **True** False

An accidental disclosure or damage to electronic records due to a natural disaster such as fire for flood or not considered reportable security incidents. True **False**

A Business Associate's verbal promise or a "handshake deal" to protect security of health information is adequate assurance under the HIPAA Security Rule.	True	**False**
A covered entity is required to define workstation use and security procedures to safeguard against unauthorized access of protected health information.	**True**	False
The only requirement for disposal of obsolete media or devices is to place such items in the recycle bin.	True	**False**
A required technical safeguard is to establish a unique user identification (such as a password) for each individual who has access to protected health information.	**True**	False
Important rules for password use include: make your password a combination of alpha-numeric characters; do not share your password; do not use an alpha or numeric series (abc-123) in your password; and do not use an easily recognized identifier such as name, birthday or address.	**True**	False

Training Outline

Sample Training Outline keyed to the HIPAA Security Standards

Administrative Safeguards (164.308)

Assigned Responsibility
Security Management Process
Workforce Security
Information Access Management
Security Awareness & Training
Security Incident Procedures
Contingency Plan
Evaluation of Plan
Business Associate Contracts

Physical Safeguards (164.310)

Facility access controls
Workstation use
Workstation security
Device and media controls

Technical Safeguards (164.312)

Access control procedures
Audit Controls
Integrity protecting information
Person or entity authentication
Transmission security

Organizational Requirements (164.314)

Business Associate Contracts
Group Health Plans

Policies Procedures and documentation (164.316)

Implement policies and procedures
Document policies and procedures

Compliance dates (164.3)

515-231