ITEM Consideration of Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policies

EXECUTIVE SUMMARY

The Health Insurance Portability and Accountability Act (HIPAA) requires that certain policies pertaining to privacy and security be in place now that the School Board is self-insured for employee health insurance. Two policies are attached for discussion at the February 12 meeting and one more concerning Information Technology will be available for consideration at the February 26 meeting along with the two attached policies. We are awaiting input from the City before finalizing that policy.

Most of the procedures required by these policies were already being followed; these policies only formalize them. In summary, it is recommended that the Board approve the HIPAA privacy and security policies on February 26, 2015.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Policies

All staff of our office with access to protected health information (PHI) shall adhere to the following policies:

Appropriate Uses and Disclosures Policy

Firewall Policy:

- We will only use health plan data for health plan related decisions.
- We will provide secure storage and computer access to records held by the health plan to minimize inappropriate access.
- We will ensure that health plan data will not be used for employment-related decisions or transferred to any non-health plan without prior written authorization by the covered individual.
- We will designate specific individuals and job classes who will have access to PHI held by the health plan. As allowed and required by law, only those individuals shall have access to this information without explicit authorization by the member or written authorization by a person duly designated to have access.

Information Requests:

- We will only respond to requests for information in writing.
- We will only respond to information requests as allowed by the regulations (treatment, payment and operations (TPO), for worker's compensation or with a properly documented request by law enforcement), when we have a properly completed and executed Authorization form for the specific information, recipient and time period requested, or if the request can be satisfied through fully de-identified data.
- We will maintain appropriate documentation of all requests. Requests for purposes of TPO do not require specific documentation.
- We will always provide only the minimum information necessary to satisfy the specific request.
- We will never release an entire member record when, in our professional judgment, a lesser amount of data would suffice.
- We will verify the source of the request and make appropriate and reasonable efforts to determine the identity of the requestor.
- We will follow protocols that may have been established regarding routine disclosures and will confer with the Privacy Officer on any other or non-routine disclosures.
- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that information requests are being handled properly and in accordance with our policies and the relevant statutes.

Self-Initiated Uses and Disclosures:

- Without proper authorization by the member, we will not initiate or allow disclosure of PHI held by the heath plan for:
    - Employment-related decisions including, but not limited to hiring, firing, job selection, and promotion decisions.
    - Use by non-health plan benefits, except as specifically allowed by law (i.e. workers compensation).

- We may initiate or allow disclosure of PHI for:
    - Workers compensation plan administration
    - A health insurance carrier or underwriter for purposes of underwriting a new contract or renewal of an existing contract for insurance.

Authorizations:

- We will always obtain a properly signed and dated Authorization form whenever needed from each member after the date that we implement HIPAA. Information requests not included under treatment, payment or healthcare operations or otherwise allowed by the regulations (disclosures for workers compensation, pursuant to a properly documented law enforcement request, and required disclosures, among others) require an authorization.
- We will not retaliate nor discriminate against members who refuse to sign an Authorization form.
- We will keep a copy of all completed information requests that are authorized by an Authorization form in the member's file.
- We will maintain Authorization forms on file for 6 years after their expiration date or event.
- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that Authorization forms are being obtained and handled properly and in accordance with our policies and the relevant statutes.
- For marketing related authorizations only, we will state in the authorization whether there was any direct or indirect remuneration to us from a third party.

De-Identification:

- We will always fulfill requests with de-identified data when, in our professional judgment, de-identified data can satisfy the request.
- We will always ensure that all 18 required elements below have been properly removed and that any remaining identifying elements cannot be used to directly retrieve member data from any other available source:
    1. Names
    2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census
        a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
        b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
    4. Telephone numbers
    5. Fax numbers
    6. Electronic mail addresses
    7. Social security numbers
    8. Member record numbers
    9. Health plan beneficiary numbers

10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that de-identified data requests are being handled properly and in accordance with our policies and the relevant statutes.

Safeguarding PHI Policy

Protecting Health Information:

- Employees must not leave member records unattended in public areas of the office.
- Employees may only access member records for which they have a legitimate, assigned business need.
- Employees may not remove files or copies of files from the office.
- Records waiting to be updated or filed must be protected. Any uncompleted work involving health data must be locked in a desk, file cabinet, or secure file room at close of business each day.

Storage and access to member records:

- Member records, including health records, will be maintained separately and secured separately from all employee records, and shall not be commingled with employment records of any kind. Any health information obtained in relation to our group health plan will be maintained separately and never be commingled with employment records. We will ensure that no health information obtained by and in relation to the health plan will be used in any employment-related decision.
- To ensure that our current paper files will be reasonably safeguarded from unauthorized public view in accordance with our policies and procedures we will, if needed, store our member files in locked filing cabinets or in a locking file room if they contain PHI or member data. Only employees with a legitimate need and authorized access for the PHI may have access to the locked area. While unattended, the file system will not be left open.
- We will make sure that archived paper files will also be secured and reasonably safeguarded which means we may, as necessary, store them in locked filing cabinets, within a locked storage area, or in a separate locked archive room. Only employees with a legitimate need and authorized access for the PHI may have access to the files. Archived member records will not reside in a general storage area except in locked file cabinets.
- Member information stored on our computers will be password protected. Only those employees with a need and authorized access to see member data will have access to the files. The computer itself will be protected as per the Technical Security Policy. Any computerized health information copied onto removable media will be protected in the same manner as paper files, as outlined above.
- Backup media that contain member data will be handled as described above for paper files, and will be handled in accordance with the Technical Security Policy.

- Any material that contains member data will, while in use, be protected from deliberate or casual oversight by passers-by. Computer screens displaying member data will be turned away from public areas so as not to be visible to passers-by in public areas. Health information waiting to be updated or filed will be secured in a locked storage cabinet or file room until the work is complete.
- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that member records are being handled properly and in accordance with our policies and the relevant statutes.

Oral Discussions:

- Employees must not discuss or share protected health data outside the office.
- Employees may not discuss any health information with other members.
- When they involve PHI, telephone conversations, discussions with members, relatives and providers will be held quietly, and as far as practical, out of the presence of passers-by.
- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that oral conversations regarding PHI are being handled properly and in accordance with our policies and the relevant statutes.

Disposal of PHI:

- Handwritten notes such as phone messages and reminder slips containing PHI must be shredded as soon as they are no longer needed.
- All unwanted or duplicate papers containing PHI must be cross-shredded immediately after it is determined that they are no longer needed.
- Diskettes, Zip Disks, tapes, re-writable CD-ROMs or any other reusable data or recording medium containing PHI or member data must be reformatted or destroyed when the data is no longer required.
- Hard drives must be reformatted when an office computer is sold, or when employees no longer use it to access PHI.
- If they contain PHI, CDs must be destroyed when the data is no longer required.
- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that member records are being disposed of properly and in accordance with our policies and the relevant statutes.

Minimum Necessary:

To maintain the confidentiality of health data, we will follow the Minimum Necessary Information principle, which minimizes the amount of PHI used and disclosed within the health care system and the number of persons who have access to this information.

The Minimum Necessary Information principle, as stated in the HIPAA regulations, is that covered entities must take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to any valid authorization received by the group health plan.
- Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
- Uses or disclosures that are required by other law.

With respect to requests for information from our business partners, we will:

- Limit the use or disclosure of, and requests for PHI (PHI) to the minimum necessary to accomplish the intended purpose.
- De-identify records if the purpose of disclosure could be reasonably accomplished with information that is not identifiable.
- Never disclose an entire member record, in response to a request for more limited data.
- Only disclose an entire member record if the request included an explanation of why the purpose of the disclosure could not reasonably be accomplished without the entire member record.
- For electronic information reviewing, forwarding, or printing out only those fields and records relevant to the user's need for information.
- For non-electronic information covered by the proposed rules, "minimum necessary" means the selective copying of relevant parts of PHI or the use of "order forms" to convey the relevant information.
- Avoid general policies of approving all requests (or all requests of a particular type) for disclosures or uses without carefully review.

In our day-to-day practices within this office, we will

- Limit the physical access that employees, business partners and others have to PHI.
- Limit the specific employees or business partners, or the types of employees or business partners, who are qualified to gain access to particular records.
- Limit computer access to appropriate portions of PHI when it is practical to do so.

Employee Education:

- For ALL employees:
- All employees of the company shall receive reminders on protecting their own health information, including that held by the group health plan. For all employees with access to member records:
    - Each employee with access to member records will receive a data privacy orientation. The employee's supervisor, the Privacy Officer, or other trainer will explain HIPAA privacy regulations as they relate to the employee's job, their importance, and how our practice has responded to these regulations.
    - Each employee with access to member records will receive a copy of all relevant policies and procedures.
    - During the orientation, the Privacy Officer, the employee's supervisor, or the trainer will discuss confidentiality of member data with the employee, and the organization and employee's obligations regarding member data confidentiality. Each employee with access to member records will sign a confidentiality statement certifying that they will not discuss or reveal any member data outside the office, and will not access or communicate any member information except as necessary to complete their assigned tasks. The confidentiality statement will include language that the obligation of confidentiality regarding member data survives the employment relationship.
    - Each employee with access to member records will sign a statement indicating that they have read, understand, and agree to abide by all privacy policies and procedures of this office, and further understand that the penalties for not following these policies and procedures may include severe disciplinary action, including termination.

- The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that all employees are trained properly regarding privacy and confidentiality and in accordance with our policies and the relevant statutes.

Individual HIPAA Rights

Alternate Communications:

- Accommodate a member's written request to receive communications involving PHI, as defined by HIPAA, at alternate locations or by alternate means.
- The request must be in writing and signed and dated by the member or their legal guardian.
- All reasonable requests shall be honored. If we feel that the request is unreasonable or we are unable to fulfill the request we will notify the member immediately.
- Once we accept the request, all communications to the member involving PHI must be made to the alternate location or by the alternate means requested until modified by the member.

Non-Routine Disclosures:

- We will accommodate a member's written request to obtain a history of non-routine disclosures of their PHI. This accounting will, at a minimum include the types of disclosures and information for each detailed under HIPAA.
- No additional accounting will be maintained by this office for valid authorizations (as defined within the HIPAA Privacy regulations) that have been received by this office. We will keep a copy of each valid authorization on file as evidence that no non-routine disclosures have been made by this office.
- If an authorization was received in relation to research disclosures we will meet the member's request for disclosure by providing a list of all protocols for which the member's PHI may have been disclosed for research pursuant to a waiver of authorization under the HIPAA Privacy regulations as well as the researcher's name and contact information.
- The request must be in writing and signed and dated by the member or their legal guardian, preferably using the History of Non-Routine Disclosures Request form.
- Every attempt will be made to satisfy the request within 30 days, but in no case will we exceed the legal requirement to complete the request within 60 days. Should this be required, we will notify the requestor in writing of the delay and the reason therefore, and complete the request in no longer than 30 additional days.
- The first request by an individual within a 12-month period shall be at no charge, additional requests shall carry a $0.25 per page duplication charge, plus applicable return receipt postage. The Privacy Officer or their representative shall notify the requesting individual of these charges in advance and provide them the opportunity to withdraw their request if they so choose.
- The report provided to satisfy the request shall use the format shown in the History of Non-Routine Disclosures Report, or contain all these data elements.
- The Privacy Officer is responsible for ensuring that all requests are fulfilled in a timely manner in accordance with the law and this office's policies.

Member Grievance and Breach of Information Privacy:

- The Privacy Officer is responsible for investigating all reported incidents of alleged violation of health information privacy, regardless of source or severity.
- All staff will encourage any individual who feels that their privacy has been violated to discuss the matter with our Privacy Officer.
- All employees will report a breach of information privacy to the Privacy Officer should they become aware of such a breach.

- The Privacy Officer will maintain a Privacy Incident File, and produce a monthly report summarizing for management the status of each and every open file regarding alleged health information privacy violations, regardless of discovering source. The Privacy Incident File shall contain:
    1. The completed Member Grievance Tracking form.
    2. The written documentation of the alleged violation by the member, staff member or other reporting entity.
    3. A Plan of Action, documenting the planned course of the investigation.
    4. Complete documentation of the investigation, including transcripts of all interviews.
    5. Documentation of all correspondence regarding the alleged violation, including all correspondence with legal counsel, such correspondence to be specifically marked as privileged communication.
    6. Documentation of the decision regarding whether or not a violation actually occurred, and any resolution regarding the alleged violation, regardless of determination. The resolution may include (upon review and approval by senior management):
        - An apology
        - A description of a process change that will prevent reoccurrence
        - An invitation to discuss the situation further
        - Addresses of appropriate professional, state and federal offices to which the complaint may be escalated
- The Privacy Officer will log all complaints in the Privacy Incident File and if the complaint can be resolved informally also document the resolution.
- If the complaint cannot be resolved informally, the individual will be asked to provide a written complaint, signed and dated.
- We will follow up with the person filing the grievance until they are satisfied or the problem is escalated.
- If the problem is escalated, the order of escalation shall be:
    1. The Privacy Officer
    2. Fiduciary and/or officer of the sponsoring organization
    3. Appropriate external professional, state or federal offices
- We will follow the current policy governing the Privacy Grievance Process and if a change is warranted, we will modify the policy documentation to reflect the change and communicate the changes to all affected staff.
- We will cooperate fully with any and all state, federal or professional investigating bodies.
- We will maintain documentation of all reported incidents for the time required by law (6 years following the last action).

Note, it is not considered a breach in any of the following instances:

- Inadvertent access of a member's medical information by someone who is normally authorized to have access to members' health information, provided that further disclosure of the information does not occur.
- Inadvertent disclosure of a member's medical information by someone who is normally authorized to have access to members' health information to another person who would normally be authorized to have access to that information, provided that further use or disclosure of the information does not occur.
- Inadvertent disclosure of a member's medical information to an unauthorized person where it is reasonable to assume that information is disclosed would not be remembered.

Non-Discrimination Policy (Preserving HIPAA Rights):

- We shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a member for exercising any of their rights under HIPAA. These include:

- The right to complain to the Department of Health and Human Services if they feel that their privacy rights had been violated.
- The right to testify in an investigation, compliance review or other hearing.
- Oppose any practice of the health plan that the individual feels is in violation of HIPAA regulations.

- We will not require individuals to waive their HIPAA as a condition of enrollment or eligibility for benefits.

Notice of Privacy Practices:

In order to notify and inform all of our members of their HIPAA rights and our responsibilities regarding their health information we shall maintain and distribute as appropriate a Notice of Privacy Practices. To that end we shall:

- Adopt and maintain on file the current Notice of Privacy Practices.
- Make available upon request paper copies of our current Notice of Privacy Practices.
- Modify the Notice of Privacy Practices as needed, with approval of senior management.
- Retain each version for not less than 6 years following the last use of that version.

Privacy Incident Instructions

Standard: An incident involving PHI is presumed to be a breach of the PHI unless **(1)** the PHI is considered secured under HHS regulations. Secured PHI means PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals under HHS guidelines, **(2)** the incident falls under the specific exclusions to the definition of a breach, or **(3)** the Privacy Officer, through the use of the following procedure, demonstrates that there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:

I. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

II. The unauthorized person who used the PHI or to whom the disclosure was made;

III. Whether the PHI was actually acquired or viewed; and

IV. The extent to which the risk to the PHI has been mitigated.

Procedure: The Privacy Officer is responsible for investigating all reported incidents of alleged violation of health information privacy, regardless of source or severity. When the Privacy Officer, another employee or an outside source reports a possible breach of privacy, the Privacy Officer will need to investigate the possible breach, determine if a breach has indeed occurred and, if so, follow up to try to prevent similar breaches from happening again. This may include sanctions or disciplinary procedures. The Privacy Incident File is simply a way for the Privacy Officer to have an organized approach to the investigation and to have all documentation of the investigation in one place. If an employee or other person becomes aware of a possible breach of health data privacy, report the alleged breach to the Privacy Officer. Then the Privacy Officer will:

1. Ask the person reporting the suspected breach to submit the details of the suspected breach in writing.
2. Review the written documentation of the alleged violation and determine if it merits further investigation.
3. If it is determined that a breach of privacy may have occurred, create a Privacy Incident File. This file will contain:
   a. The Privacy Incident File Summary.
   b. The written documentation of the alleged violation as originally reported.
   c. A plan of action, documenting the planned course of the investigation.

d. Complete documentation of the investigation, including transcripts of all interviews.

e. Documentation of all correspondence regarding the alleged violation, including all correspondence with legal counsel, such correspondence to be specifically marked as privileged communication.

f. Documentation of the decision regarding whether or not a violation actually occurred, and any resolution regarding the alleged violation, regardless of determination.

4. Investigate what was done to contain the breach once it was detected.
5. Analyze the seriousness of the problem and decide what level of breach has occurred:
   a. Very serious - a large amount of data, or very sensitive data has been made public
   b. Serious - a large amount of data has potentially been exposed, but the likelihood of it being accessed is small
   c. Important - protected member data has been inappropriately released to a trusted business partner, but the likelihood of further exposure is very low
   d. Minor - protected member data has been handled carelessly but no exposure occurred.
6. Decide the level of culpability:
   a. Very serious - malicious action on the part of an employee or outsider
   b. Serious - employee willfully ignored established policies
   c. Important - employee inadvertently failed to follow established policies
   d. Minor - an error in judgment caused by unclear policies
7. Document what data or physical assets may have been compromised, destroyed or stolen.
8. Develop a detailed plan of action (summarize on the Privacy Incident File Summary):
   a. Decide how to proceed with the investigation to determine the true cause of the breach and whether policies or procedures need to be changed to preclude future breaches.
   b. Include supervisory or management personnel in the process as appropriate.
   c. In a serious or very serious situation include your lawyer in the planning.
   d. With a serious or very serious situation involve professional, state and/or HIPAA oversight agencies.
   e. If the breach occurred through outside interference, notify the police.
   f. With a serious or very serious situation contact each individual whose PHI either has been or is reasonably believed to have been compromised by the breech.
      I. This notice shall be written in plain language and sent out no later than 60 days following the discovery of the breach by first-class mail.
      II. In the case where there is insufficient or out-of-date contact information then an alternate means of contacting the individuals involved must be used.
         A. If there are fewer than 10 individuals needing an alternate notice, then notice may be made using an alternate written notice (such as e-mail), by telephone, or other appropriate means.
         B. If there are more than 10 individuals needing an alternate notice, then the alternate notice must be posted conspicuously on our web site for at least 90 days or be posted in major print or broadcast media where the individuals are likely to reside and must include a toll-free number to call for more information (active for at least 90 days).
      III. If notice is deemed to be urgent due to the imminent misuse of the data, individuals may be contacted by phone, e-mail or other means in addition to the written notice.

g. If the breach affects more than 500 members' health information, the Privacy Officer shall also notify prominent news outlets serving the state or local area of the breach within 60 days.

h. The Privacy Officer shall also notify the US Department of Health and Human Services (HHS) that a breach has occurred:

   I. If the breach affects more than 500 members' health information, notification of the breach must be made at the same time that individual members are notified.

   II. If the breach affects less than 500 members' health information, the Security Officer may choose to keep a log of the breach and report all such breaches annually to HHS within 60 days after the end of the calendar year.

i. Notice to individuals, the media (if appropriate) and to HHS must be delayed if a request is received from law enforcement that the notice may impede a criminal investigation or national security. The delay may be no more than 30 days unless the request is in writing and includes the anticipated length of the delay.

j. Decide on appropriate consequences for any responsible employee.

k. Decide if policies need to be added or modified to prevent reoccurrence.

9. Add the plan of action to the Privacy Incident File.
10. Document the progress and outcome of the investigation in the Privacy Incident File.
11. Discharge and document any sanctions and disciplinary actions.
12. Add or modify policies and re-train employees as appropriate to prevent reoccurrence.
13. Cooperate with any resulting professional, state or federal investigation.

Violation of these policies can carry serious consequences for the group health plan. Disciplinary actions for anyone violating this policy may include suspension without pay or termination.

Health Insurance Portability and Accountability Act (HIPAA) Security Policies

Facility Security Policy

Facility Security:

HIPAA requires a plan for securing the physical facilities of the office. Our office is committed to providing a safe work environment and to ensuring the security of protected health information (PHI) entrusted to us, as well as our equipment and other valuables.

Lock Doors

All exterior doors shall be locked at our posted closing time or when the last person leaves the office. Doors leading to health plan-only areas or those otherwise designated as not accessible by non-health plan employees shall be locked when the area is not in use (unless locking these creates a fire hazard). No door that is to remain locked shall be propped open under any circumstances.

Keys and other access devices (card keys, badges, etc.) shall only be available to those with a legitimate need based on management's written approval. Under no circumstances shall access devices be lent, copied or otherwise transferred except with the written approval of management. Loss or theft of any access device shall be reported promptly to the Security Officer.

Visitor Policy

Any non-employee who needs to be in any part of the office usually reserved for employees only shall be escorted to the area they need to visit, once we determine that they have a legitimate need to be there, and shall not be allowed to wander unattended. Any non-employee whom we notice outside of the area where we expect them to be shall be challenged and asked to return to the area where they belong.

After Hours Admission

No employee shall, without prior approval of management, gain admission to the office outside of his or her work hours for purposes other than to conduct the business of the health plan.

Periodic Review

The Security Officer will conduct a periodic review of the physical security of the facilities using the Facility Security Checklist. These reviews should be conducted monthly and the results recorded on the checklist. All problems must be dealt with promptly.

Facility Security Maintenance:

It is the policy of our office that any modifications, alterations, repairs or other changes to the physical space of this office that include the following items be logged as of the start of the modification:

- Doors
- Windows
- Locks
- Alarms and alarm systems (including any related communications lines)
- Walls
- Roof/Ceiling
- Interior Walls
- Wiring
- Office equipment used as a room divide

Tracking and Control of Protected Health Information:

1. Under no circumstances will ANY PHI be transmitted without the appropriate safeguards in place to protect our members' health information or when required to, obtain an Authorization form to keep on file, or unless the information has been de-identified.
2. Routine movement of electronic PHI will be logged on the "PHI Tracking Log – Routine" stating the details of the transfer.
3. Each non-routine movement of electronic PHI will be logged on the "PHI Tracking Log – Non-Routine" stating the details of the transfer.
4. The Security Officer is responsible for ensuring that this policy is followed diligently.
5. All Records Handling Logs will be retained for six years following the last dated entry.

HIPAA Personnel Security Policy

Personnel Screening:

The Security Officer is responsible for ensuring that all employees that work with member data, or in the areas where member data is stored or used, will be properly screened, trained and supervised. These responsibilities include

1. Supervision – assuring supervision of people who do not have a need to access electronic member data when those people are working or waiting in an area where member data may be stored or exposed.
2. Maintaining a record of access authorizations – ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.
3. Establishing personnel clearance procedures in conjunction with the health plan's attorney.
4. Assuring that system users, receive security awareness training.

PHI Access:

1. The Security Officer is responsible for determining whether an employee or business associate is allowed access to member data. Those who may have access will:
   - Have a legitimate business need to access the data,
   - Have signed a confidentiality or business associate agreement,
   - Are aware of and agree to adhere to all HIPAA privacy policies, and
   - Agree absolutely not to share their account access.
2. The Security Officer is responsible for coordinating the limitation of member data access by employees and business associates to the minimum level of information necessary to accomplish their defined tasks. This includes:
   - Admission to secure parts of the building,
   - Password access to workstations and servers,
   - Password access to applications or parts of applications,
   - Ability to run selected reports,
   - Ability to send or receive transactions via modem, and
   - Ability to access the Internet.
3. The Security Officer is responsible for coordinating the modification of a user's access to member data. Access should be evaluated for modification when
   - A user's job responsibilities change,
   - New or upgraded application software allows greater control of application access,
   - New or upgraded system software provides greater control of hardware or process access, or
   - A user or business associate has been terminated.

4. The Security Officer will obtain the approval of a senior manager of the health plan regarding all data access level determinations.
5. The Security Officer will be responsible (with the assistance of the Information Technology Department) for monitoring system logins, file access and security incidents associated with the member data stored on or transmitted by your computer system. These responsibilities include:
    - Use and regular review of system traces appropriate to the level of complexity of the computer system,
    - Use and regular review of audit functionality available through the application software, and
    - Creation and maintenance of a Security Incident File.

Sanctions:

1. The Security Officer is responsible for investigating (with the assistance of the Compliance Department) all reported incidents of alleged violation of member information security, regardless of source or severity, and applying appropriate sanctions to violators.
2. The Security Officer will complete a Security Incident Report for each alleged incident.
3. If the Security Officer determines that a breach occurred, they will assess the seriousness of the breach and apply appropriate sanctions:
    - Very serious – malicious action on the part of an employee
    - Serious – employee willfully ignored established policies
    - Important – employee inadvertently failed to follow established policies
    - Minor – an error in judgment caused by unclear policies or misunderstanding
4. Disciplinary actions for violation of member information security could include: additional training, verbal or written warnings, suspension without pay or termination of employment.
5. We will cooperate fully with any and all state, federal or professional investigating bodies if appropriate.

Employee Security Orientation:

For ALL employees:

- All employees of the company shall receive reminders on protecting their own health information, including that held by the group health plan.
- For all employees with access to member records:
    - Each employee with access to member records will receive a data security orientation. The employee's supervisor or other trainer will explain HIPAA security regulations as they relate to the employee's job, their importance, and how our practice has responded to these regulations.
    - Each employee with access to member records will receive a copy of all relevant policies and procedures.
    - During the orientation, the Security Officer, the employee's supervisor or the trainer will discuss the security procedures in place to protect member data with the employee, and the organization's and employee's obligations regarding patient confidentiality.
- The Security Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that employees are trained properly regarding privacy and confidentiality and in accordance with our policies and the relevant statutes.
- All new employees shall receive the same training as existing employees: summary training for all employees and a full security orientation for those new employees with access to member records.

Termination:

1. In the event of the termination of any employee or business associate that has had access to any form of PHI retrieve all physical security tokens, keys, access cards, etc. that could be used to gain access to the premises or data of this organization.
2. At the time that the various physical security access devices are retrieved, or during an exit interview, the Security Officer or their designated representative will make every effort possible to obtain the signature of the employee or business associate that is being terminated on the Termination Security Checklist and its incorporated statement regarding the on-going need to maintain confidentiality of member PHI. Barring that, the Security Officer or their representative must discuss with the terminated

person the need to continue to maintain confidentiality regarding member records, and note that a signature could not be obtained, with a reason for not obtaining it.

3. The Security Officer is responsible for ensuring that this policy is followed diligently.
4. All Termination Security Checklists will be retained for six years.

Security Incident Procedure

Standard: An incident involving PHI is presumed to be a breach of the PHI unless (1) the PHI is considered secured under HHS regulations. Secured PHI means PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals under HHS guidelines, (2) the incident falls under the specific exclusions to the definition of a breach (see below), or (3) the Security Officer, through the use of the following procedure, demonstrates that there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:

I. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
II. The unauthorized person who used the PHI or to whom the disclosure was made;
III. Whether the PHI was actually acquired or viewed; and
IV. The extent to which the risk to the PHI has been mitigated.

Procedure: This step-by-step procedure will be followed explicitly and completely whenever an actual or attempted breach of physical or electronic security has occurred.

1. Report the attempted or actual breach to the Security Officer. If the breach is physical, secure the area, but do not touch anything, as physical intrusions may be part of a crime scene.
2. The Security Officer will move immediately to contain the breach and minimize the damage to the organization, its data, and its physical assets.
3. The Security Officer will document the breach and conduct or direct all follow-up activity.
4. The Security Officer will contact law enforcement authorities if there is indication of criminal conduct or theft involved.
5. The Security Officer will conduct a risk analysis to determine whether:
   a. All PHI had been secured properly in accordance with specified HIPAA standards; and
   b. Despite the breach there is a low probability that PHI has been compromised.
6. After completing the risk analysis, if the Security Officer determines that PHI had not been secured properly or that there is more than a low probability that PHI was compromised, notice of the breach must be made to the following:
   a. Each individual whose PHI either has been or is reasonably believed to have been compromised:
      i. This notice shall be written in plain language and sent out no later than 60 days following the discovery of the breach by first-class mail.
      ii. In the case where there is insufficient or out-of-date contact information then an alternate means of contacting the individuals involved must be used.
         A. If there are fewer than 10 individuals needing an alternate notice, then notice may be made using an alternate written notice (such as e-mail), by telephone, or other appropriate means.
         B. If there are more than 10 individuals needing an alternate notice, then the alternate notice must be posted conspicuously on our web site for at least 90 days or be posted in major print or broadcast media where the individuals are likely to reside and must include a toll-free number to call for more information (active for at least 90 days).
      iii. If notice is deemed to be urgent due to the imminent misuse of the data, individuals may be contacted by phone, e-mail or other means in addition to the written notice.
   b. If the breach affects more than 500 members' health information, the Security Officer shall also notify prominent news outlets serving the state or local area of the breach within 60 days.
   c. The Security Officer shall also notify the US Department of Health and Human Services (HHS) that a breach has occurred:

   i. If the breach affects more than 500 members' health information, notification of the breach must be made at the same time that individual members are notified.
   ii. If the breach affects less than 500 members' health information, the Security Officer may choose to keep a log of the breach and report all such breaches annually to HHS within 60 days after the end of the calendar year.
7. Notice to individuals, the media (if appropriate) and to HHS must be delayed if a request is received from law enforcement that the notice may impede a criminal investigation or national security. The delay may be no more than 30 days unless the request is in writing and includes the anticipated length of the delay.
8. The Security Officer will, in a timely manner, complete a Security Incident Report, including follow-up and recommendations, and log the incident on the Security Incident Log.
9. The Security Officer will, in a timely manner, report the incident to senior management and make appropriate recommendations to correct the policies, procedures, and/or technological solutions necessary to prevent a recurrence.

Note, it is not considered a breach in any of the following instances:

1. Inadvertent access of a member's medical information by someone who is normally authorized to have access to members' health information, provided that further disclosure of the information does not occur.
2. Inadvertent disclosure of a member's medical information by someone who is normally authorized to have access to members' health information to another person who would normally be authorized to access to that information, provided that further use or disclosure of the information does not occur.
3. Inadvertent disclosure of a member's medical information to an unauthorized person where it is reasonable to assume that information is disclosed would not be remembered.