Everett School Employee Benefit Trust

HIPAA Security Policy

I. Introduction

Everett School Employee Benefit Trust ("Trust") provides one or more group health plans subject to HIPAA's security regulations (collectively the "Group Health Plan") for eligible employees of the Everett School District ("District"). The Group Health Plan is sponsored by the District and the Everett Education Association (collectively the "Plan Sponsor"). Members of the District's workforce may create, receive, maintain, or transmit certain limited amounts of electronic protected health information (as defined below) on behalf of the Plan Sponsor, for plan administration functions.

The Group Health Plan is subject to the security rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing administrative simplification security regulations ("Security Rules").

Most of the Group Health Plan is provided pursuant to insurance policies issued by insurance companies ("Health Insurance Issuers"). Almost all of the electronic protected health information of the Group Health Plan resides with these Health Insurance Issuers, which are also subject to HIPAA and the Security Rules. This policy is complementary and supplementary to the HIPAA security policies of the Health Insurance Issuers. To the extent that PHI (defined below) is under the control of a Health Insurance Issuer, and has not been disclosed or released to any member of the District's workforce, the Health Insurance Issuer has primary responsibility for compliance with the Security Rules.

The purpose of this document is to set a policy for the Group Health Plan to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") security regulations concerning electronic protected health information, which are found at 45 C.F.R. Parts 160 and 164. HIPAA and its implementing regulations require the Group Health Plan to implement various security measures with respect to electronic protected health information ("ePHI").

It is the Group Health Plan's policy to comply fully with the requirements of HIPAA's security regulations. No third-party rights (including, but not limited to, rights of Group Health Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Group Health Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Group Health Plan. This Policy does not address requirements under state law or federal laws other than HIPAA.

II. Definitions

A. *Electronic Protected Health Information or ePHI* is protected health information that is transmitted by or maintained in electronic media.

B. *Protected Health Information or PHI* is the information that is subject to and defined in the Group Health Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to in this Policy as "Exempt Information":

1. summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Group Health Plan;

2. enrollment and disenrollment information concerning the Group Health Plan which does not include any substantial clinical information;

3. health information which has been de-identified in accordance with HIPAA's privacy rules; or

4. PHI disclosed to the Group Health Plan and/or District under signed authorization that meets the requirements of the HIPAA privacy rules.

C. *Electronic Media* means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

III. Security Official

Molly Ringo is the Security Official for the Group Health Plan. The Security Official is responsible for the development and implementation of the Group Health Plan's policies and procedures relating to security, including but not limited to this Policy. The Security Official also shall hear all complaints regarding alleged violations of this Policy and shall ensure that the complaint and its disposition are appropriately handled and documented.

IV. Risk Analysis

The Group Health Plan, in connection with the District's Human Resources Department, has undertaken a risk analysis to assess the potential vulnerabilities and risks to the confidentiality, integrity and availability of ePHI, with the following results:

The Group Health Plan has no employees. The Trustees of the Trust are not involved in the appeals of claim denials or in any other capacity concerning the processing of claims. All of the Group Health Plan's functions, including creation and maintenance of its records, are carried out by the Health Insurance Issuers, business associates of the Group Health Plan, and to a small extent, employees of the District's Human Resources Department. The Group Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit ePHI relating to the Group Health Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Health Insurance Issuers, other business associates, and to a limited extent, the District. Accordingly, Health Insurance Issuers, the business associates of the Group Health Plan or the District: (1) create and maintain all of the ePHI relating to the Group Health Plan; (2) own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit ePHI relating to the Group Health Plan, and (3) control their employees, agents, and subcontractors who have access to ePHI relating to the Group Health Plan. The Group Health Plan has no or limited ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI being held by the Health Insurance Issuers and business associates.

Because the Group Health Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Health Insurance Issuers and business associates affecting the security of the Group Health Plan ePHI, the Health Insurance Issuers and business associates have undertaken certain obligations relating to the security of ePHI that they handle in relation to the performance of administration functions for the Group Health Plan, the Group Health Plan's policies and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 CFR Part 164, except in conjunction with the District's Human Resources Department, as described in Section VIII of this Policy:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the Health Insurance Issuers and business associates for ePHI of the Group Health Plan for the standards listed above, as well as the policy under these procedures as set forth in Section VIII of this Policy, are adopted by the Group Health Plan.

V. Group Health Plan Document: Plan Sponsor's Safeguards

The Group Health Plan documents include provisions requiring the Plan Sponsor to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Group Health Plan ("Plan's ePHI");
- ensure that reasonable and appropriate security measures support the Group Health Plan document provisions providing for adequate separation between the Group Health Plan and the Plan Sponsor;
- ensure that any agents or subcontractors to whom the Plan Sponsor provides the Plan's ePHI agree to implement reasonable and appropriate security measures to protect the Plan's ePHI; and
- report to the Security Official any security incident of which the Plan Sponsor becomes aware.

VI. Risk Management

The Group Health Plan manages risks to its ePHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Group Health Plan;
- The Group Health Plan's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the ePHI potentially affected.

Based on risk analysis discussed in section IV of this Policy, the Group Health Plan has made a reasoned, well-informed, and good-faith determination on the implementation of the HIPAA security regulations that the Group Health Plan need not take any additional security measures, other than the measures set forth herein and the measures adopted to reduce risks to the confidentiality, integrity and availability of ePHI: (a) in conjunction with the Human Resources Department of the District as described in Section VIII; and (b) by the Health Insurance Issuers and business associates of the Group Health Plan.

VII. Disclosures of ePHI to Business Associates

A business associate is an entity (other than the Plan Sponsor), or a Health Insurance Issuer, that:

- performs or assists in performing a Group Health Plan function or activity involving the use and disclosure of PHI (including data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

The Group Health Plan permits business associates to create, receive, maintain, or transmit ePHI on its behalf. The Group Health Plan has obtained or will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA privacy and security regulations and specifically providing that the business associate will:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of all of the Plan's ePHI that the business associate creates, receives, maintains, or transmits on behalf of the Group Health Plan;
- ensure that any agents or subcontractors to whom the business associate provides the Plan's ePHI agree to implement reasonable and appropriate security measures to protect the Plan's ePHI;
- take required steps with respect to notification requirements concerning breaches of unsecure PHI;
- report to the Group Health Plan any security incident of which the business associate becomes aware; and
- authorize termination of the contract by the Group Health Plan, if the Group Health Plan determines that the business associate has violated a material term of the contract.

In addition to these requirements being contractual obligations of the business associate under the written contract, a business associate of the Group Health Plan is required under federal law and independent of such written contract to comply with the HIPAA security regulations to protect the security of the ePHI the business associate creates, receives, maintains, and transmits on behalf of the Group Health Plan. Thus, the Group Health Plan can reasonably rely that its business associates will comply with the HIPAA security requirements pursuant to applicable federal law.

VIII. HIPAA Security Compliance Measures for Group Health Plan in Conjunction with District's Human Resources Department

Certain employees of the District may have limited access to ePHI of the Group Health Plan for plan administration and other permissible purposes, via access to secure servers of the Health Insurance Issuers or other secure means. If available, access to these secured servers is password-protected, and only certain members of the Human Resources Department have passwords to access these servers. To an even more limited extent, it is possible that ePHI may be communicated via the District's email system, and such ePHI is stored and used on District computers and other electronic media. The Group Health Plan, in conjunction with the District's Human Resources Department, has undertaken necessary and appropriate steps, as described in this Section VII, to protect the security of the Plan's ePHI which is created, received, maintained, or transmitted by the Human Resources Department ("HR Department") employees.

A. Administrative Safeguards.

1. Security Management Process. The following policies and procedures regarding security management of ePHI are adopted:

   a. *Risk Analysis.* The following is a description of the risk analysis undertaken to assess the potential vulnerabilities and risks to the confidentiality, integrity and availability of the Plan's ePHI being used or held by certain District employees. The Health Insurance Issuers for the Group Health Plan create, receive, maintain and transmit the vast majority of Plan ePHI. A small amount of ePHI may be created, received, maintained or transmitted by the District is email in Microsoft Outlook ("Outlook") on the computers of employees of the HR Department and the District's wellness coordinator ("HR Employees"). The risks and vulnerabilities to this email in Outlook are very minimal. For confidentiality issues, there is a very low risk that unauthorized persons can access the material because unique passwords are required to access the email of these employees in Outlook, firewalls are in place to prevent hacking into the District's computer system and because of the physical security at the District's worksite. Software runs continuously on the District systems to scan emails to protect against viruses, worms and similar issues. Concerning integrity and availability, the ePHI in Outlook is not generally not critical or essential to the day-to-day workings of the Group Health Plan, which is operated and maintained by off-site Health Insurance Issuers and other business associates. If a computer holding ePHI at the District crashed, the ePHI in Outlook can generally be recreated or obtained from the Health Insurance Issuer or other source. In addition, a complete failure or crash of a District computer which would result in the destruction of the ePHI in Outlook would be extremely rare. For the same reason, there is little concern to the Group Health Plan if there was a fire or natural disaster at the District which destroyed the ePHI because the ePHI is also in the hands of the Group Health Plan's Health Insurance Issuers. The District has in place reasonable and appropriate measures to control passwords and to protect against viruses and worms.

   b. *Risk Management.* The following security measures are in place to reduce risks and vulnerabilities to the ePHI in Microsoft Outlook.

      i. The District's Human Resources' department is not open to the general public. Visitors or non-Department employees must be escorted by HR Employees.

      ii. HR Employees with access to ePHI are required to protect their passwords from other employees and from visitors by storing their passwords in secure locations.

      iii. Computers for the HR Employees have in place a mechanism by which the computer will lock-down after a period of 10 minutes of non-use.

      iv. Temporary employees will not be hired to fill HR Employee positions unless the temporary employees are fully trained regarding this policy and the HIPAA privacy policies relating to the Group Health Plan. Temporary employees will be screened to determine whether access to ePHI should be granted to them.

      v. In addition, the HR Department and the Group Health Plan will continue to implement other security measures already in place and described in the previous section, Risk Analysis, to protect the ePHI of the Group Health Plan.

c. *Sanction Policy.* District employees who violate this policy are subject to disciplinary action, including, but not limited to, reprimands and termination.

d. *Information System Activity Review.* On a periodic basis, the HR Department or a representative of the Group Health Plan will review records of information system activity, especially activity in Outlook, such as audit logs or access reports, to determine if security violations relating to the ePHI have occurred. The results of these reviews will be documented and kept in a secure file with the Security Official.

2. Workforce Security. The following policies and procedures regarding workforce security are adopted:

a. *Authorization and/or Supervision.* Outside visitors and employees of other departments of the District are not authorized to be in the HR Department workplace unless they are supervised by HR Employees, who are trained not to allow unauthorized access to ePHI. HR Employees are required to monitor their workstations so that unauthorized employees or guests do not inadvertently view or have access to ePHI of the Group Health Plan. Computers of HR Employees are protected by unique user identification and passwords. HR Employees are required to log off of their computers or turn their computers off at night when cleaning crews are in the area.

b. *Workforce Clearance Procedures*. Only HR Employees work on a daily basis with ePHI of the Group Health Plan. There is a screening process, which includes a background check in the hiring process, to determine that access to ePHI is appropriate for these employees. HR Employees only have access to ePHI for purposes of administration of the Group Health Plan.

c. *Termination Procedures*. Access to ePHI will be terminated as soon as practicable when an HR Employee's employment at the District terminates. When an HR Employee leaves the employment of the District, the employee is required to turn in all keys, badges and passcards for access to the building and to their previous workplaces. The entire accounts for such terminated employees, including passwords and unique user identifications, are immediately disabled on the District's computer systems. Health Insurance Issuers and business associates are informed about terminated employees and are instructed to disable passwords of the terminated employees to their secure servers.

3. Information Access Management. The following policies and procedures regarding information access management are adopted.

a. *Isolating Healthcare Clearinghouse Functions*. This standard does not apply to the Group Health Plan.

b. *Access Authorization*. Only HR Employees have access to ePHI on a regular basis. Other personnel, such as those responsible for the District's computers, are only granted access to ePHI on a very limited and "as needed" basis for issues dealing with the computer of an HR Employee. Any access to ePHI granted to non-HR Employee District personnel is also only the minimum necessary to accomplish the particular necessary task or function.

c. *Access Establishment and Modification*. Only HR Employees have access to ePHI on a regular basis. If an HR Employee is transferred outside of the HR Department, the Plan's Security Official and/or supervisory employees in the HR Department will take appropriate steps to block further access to ePHI of the Group Health Plan, including removing these files from Outlook Exchange for the employee and terminating their passwords to secure servers of the Health Insurance Issuers or business associates.

4. Security Awareness Training. The following policies and procedures regarding security awareness training are adopted.

   a. *Security Reminders*. HR Employees receive initial and continuing training in HIPAA security rules and this policy, as directed by the Security Official. The Security Official will periodically send emails or other communications reminding them of the rules and this policy, and will ensure that new HR Employees receive training as needed.

   b. *Protections from Malicious Software.* The District's computers and computer networks and systems, including those used by the HR Employees, have protections against viruses and worms and similar malicious software programs. These protections are updated on a periodic basis. HR Employees may not install unauthorized software on their computers at work.

   c. *Log-in Monitoring*. After three attempts, District computers will not grant access to an individual user if the user attempts to enter the system and does not enter the correct password. In this instance, the employee in question must obtain a new password in order to operate the computer at his or her desk. Issues and discrepancies relating to log-in monitoring success and failures are reported to the Security Official.

   d. *Password Management.* Passwords to the computers of the HR Employees have certain characteristics that make them difficult to duplicate. All passwords are required to be changed every 90 days. HR Employees may not share their passwords with other employees and may not have passwords easily accessible at their workstations.

5. Security Incident Procedures. The following policies and procedures regarding security incidents are adopted.

   a. *Response and Reporting*. All HR Employees are required to report any security incidents to the Security Official for appropriate investigation and action. For purposes of this Policy, a security incident is any attempted or successful unauthorized access, use, disclosure, modification of destruction of information or interference with system operations in the District computers which would involve ePHI. The Security Official will respond to security incidents and will document the security incidents and outcomes. To the extent practicable, the Security Official will take steps to mitigate the harmful effects of the security incidents which are reported to the Security Official.

6. Contingency Plan. The following contingency plans and policies are adopted.

   a. *Data Backup Plan*. The District has a data backup plan which applies to the ePHI held on the HR Department computers. In addition, since the Group Health Plan is run by Health Insurance Issuers, most of the ePHI of the Group Health Plan could be retrieved from the Health Insurance Issuers or from the person or entity that sent the email to or received the email from the HR Department. The ePHI at the Health Insurance Issuers' offices is subject to the data backup plans of the Health Insurance Issuers.

   b. *Disaster Recovery Plan.* A disaster at HR Department offices would not effect in any large measure the day-to-day operations of the Group Health Plan. In the event of a disaster at the offices, essential ePHI would be obtained from data backup sources, from providers, from the Health Insurance Issuers and from other sources. The Group Health Plan is also relying on, and would utilize, the disaster recovery plans of the Health Insurance Issuers for the Group Health Plans.

c. *Emergency Mode Operation Plan.* In an emergency, the Group Health Plan would be operated, as it is now, through off-site Health Insurance Issuers and business associates. The HR Department offices, and the computers within the offices, would be protected by security for the site. The Group Health Plan is also relying on the emergency mode operation plans of its Health Insurance Issuers for the Group Health Plan.

d. *Testing and Revision Procedures.* The District conducts fire drills and similar types of testing at the HR Offices.

e. *Periodic Review.* The Group Health Plan will conduct periodic reviews of its contingency plans to determine whether revisions are necessary or desirable.

f. *Applications and Data Criticality Analysis*. The most critical applications for ePHI are Outlook and the firewall software (i.e., the virus and worm protection software) utilized by the District.

7. Evaluation. The following policies and procedures regarding evaluation of its security safeguards are adopted.

a. *Periodic Technical and Non-Technical Evaluation*. The Trustees of the Trust and the HR Department will conduct periodic evaluations (technical and non-technical) of its security safeguards to determine the continued protection of the ePHI of the Group Health Plan and to determine if new risks may be present. Such evaluations are appropriate when new technology, new risks or other changes to the security environment occur.

B. Physical Safeguards.

1. Facility Access Controls. The following policies and procedures regarding facility access controls are adopted.

a. *Contingency Operations.* In an emergency, the Group Health Plan would be operated, as it is now, through the Health Insurance Issuers. The District offices, and the computers within the offices, would be protected by security. In emergency situations, the HR Employees and the Security Official first will be granted access to the ePHI and will determine the extent to which access for other personnel is appropriate. Any critical data which is lost would be recovered from the Health Insurance Issuers and/or from other persons who sent the email to or received the email from the HR Employees.

b. *Facility Security Plan*. The District offices have a facility security plan. Most doors to the building have controlled entrances which require keys for entrance. Visitors to the building must check in and be escorted by District employees. Any unauthorized entries are immediately reported to security personnel or as necessary to the Everett police department and other law enforcement officials.

c. *Access Control and Validation Procedures*. Visitors to the District offices are escorted by District employees. Employees of other departments are not authorized to be in the Human Resources workplace unless they are supervised by HR Employees. Computers housing ePHI are protected by passwords. Computers are logged off or turned off at night when cleaning crews or other maintenance personnel are in the Human Resources department.

d. *Maintenance Records.* The Security Official will document repairs and modifications to the physical components of the security systems which relate to ePHI of the Group Health Plan.

2. Workstations Use and Workstations Security. The following policies and procedures regarding workstations use and security are adopted.

a. *Proper Functioning and Physical Attributes of Workstations, Physical Safeguards for Workstations.* District employees who are not employees of the HR Department are not authorized to be in the HR Department or to view the computers of HR Employees, unless such non-HR Department employees are adequately and properly supervised. Access to HR Employee workstations is controlled by unique user identification codes and passwords. HR Employees are required to log off of their computers at the end of the work day and when they are going to be away from their workstations for extended periods of time during the work day. See also the policies for Facility Security Plan. HR Employees are not authorized to access email with ePHI when they are off-site.

3. Device and Media Controls. The following policies and procedures regarding device and media controls are adopted.

a. *Proper Disposal of PHI and Hardware/Software Storing PHI.* Before disposal of a computer in the HR Department, the Security Official or her designee shall insure that all ePHI in the computer is completely removed from the computer. Before such removal of the ePHI, any essential ePHI on the computer will be retrieved and stored elsewhere if it is not otherwise available.

b. *Media Re-Use*. Before re-use of a HR Department computer by another District department, all ePHI on the computer is completely removed from the computer in a manner which makes its re-creation by a new user impossible. If ePHI is stored on CD, floppy discs or other similar electronic media, the ePHI will be completely removed prior to re-use of the electronic media, or the electronic media will be destroyed and not re-used. If ePHI is stored on CD, floppy discs or other similar electronic media, the media will be store in locked file cabinets.

c. *Accountability.* The District maintains a record of all District computers by serial number and a log of the location of these computers.

d. *Data Backup and Storage*. Appropriate steps will be undertaken to create a copy of essential ePHI on the computers of HR Employees if the computers are moved and such movement creates a risk of losing data or a risk to the integrity of the data.

C. Technical Safeguards.

1. Access Controls. The following policies and procedures regarding access controls are adopted.

a. *Unique User Identification*. There is an assigned unique user name for identifying and tracking the identity of users of the HR Department computers, along with passwords. All passwords are required to be changed every 90 days. It is violation of this policy for HR Employees to allow another person access to or to use the HR Employee's unique user identifications and/or passwords. All HR Employees must ensure that their passwords are not documented, written, or otherwise exposed in an insecure manner. If an HR Employee has a reason to believe that his or her user identification or password has in any way been compromised, he or she must report that security incident to the Security Official.

b. *Emergency Access Procedure*. In the event of an emergency, ePHI of the Group Health Plan will be obtained through the Health Insurance Issuers of the Group Health Plan. If the emergency extends to the Health Insurance Issuers' offices or facilities, the Group Health Plan will follow the emergency access procedures adopted by the Health Insurance Issuers.

c. *Automatic Logoff*. The computers of HR Employees have an automatic logoff feature.

d. *Encryption.* Because of the small amount of ePHI transmitted to or from or held at the HR Department, it is not reasonable and practical to encrypt ePHI (such as emails to other service providers or plan participants). If any such other PHI is of an extremely sensitive nature, it will be communicated via non-electronic means (such as dedicated fax lines).

2. Audit Controls. The following policies and procedures regarding audit controls of the ePHI are adopted.

a. *Record Internal Uses of PHI by User.* The District has in place computer programs which allow the District to record and examine activity by users.

3. Integrity. The following policies and procedures regarding integrity of ePHI are adopted.

a. *Mechanism to Authenticate ePHI.* The official records of the Group Health Plan are held in the possession of the Health Insurance Issuers, so the Group Health Plan relies on them to implement electronic mechanisms to corroborate that the Plan's ePHI has not been altered or destroyed in an unauthorized manner. The likelihood of tampering with emails in Outlook at the HR Department is minimal and in any instances where tampering might have occurred, the HR Employees will authenticate the ePHI with the Health Insurance Issuer or the provider of the medical services.

4. Person or Entity Authentication. The following policies and procedures regarding person or entity authentication are adopted.

a. *Person/Entity Seeking Access is the One Claimed.* The HR Department utilizes unique user ID and passwords to verify that persons seeking access to ePHI are the employees authorized to gain such access.

5. Transmission Security. The following policies and procedures regarding the security of transmissions of ePHI are adopted.

a. *Integrity Controls*. Most of the ePHI obtained by HR Employees is located on secured servers from Health Insurance Issuers for the Group Health Plans. Communication with them is password or otherwise protected.

b. *Encryption.* Most of the ePHI obtained by HR Employees is ePHI transmitted to and from the Health Insurance Issuers. Communication with them is conducted via a secure server or via other secure means. Because of the small amount of other ePHI transmitted to or from or held at HR Employees, it is not reasonable and practical to encrypt the other ePHI (such as emails to other service providers or plan participants). If any such other PHI is of an extremely sensitive nature, it will be communicated via non-electronic means (such as dedicated fax lines). For this small amount of other ePHI, the Group Health Plan has determined that this is a reasonable and practical alternative to encryption, given the technical and financial burdens associated with encryption.

D. Breaches of Unsecured PHI.

The Group Health Plan will comply with the requirements of HIPAA and implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Group Health Plan, a Health Insurance Issuer or a business associate discovers a breach of unsecured PHI.

IX. Documentation

The Group Health Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Group Health Plan ePHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by the HR Employees or business associates, the Group Health Plan shall document certain actions, activities, and assessments with respect to ePHI required by HIPAA to be documented (including amendment of the Group Health Plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the Group Health Plan may be maintained in either written or electronic form. The Group Health Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Group Health Plan will make its policies, procedures, and other documentation available to the Security Official and the Plan Sponsor, Health Insurance Issuers, and business associates or other persons responsible for implementing the procedures to which the documentation pertains.