Louisiana Sheriffs' Association

Health & Welfare Plan

Policies & Procedures

Health Insurance Portability & Accountability Act (HIPAA)

As Amended by the

Health Information Technology for Economic Clinical Health Act (HITECH)

Table of Contents

Introduction

These are the Privacy Policies and Procedures of Louisiana Sheriffs' Association Health and Welfare Plan (the "Plan"). HIPAA Privacy Policies and Procedures were effective as of **July 1, 2017**.

Administrative Privacy Protections

Policy

The Plan shall have in place certain administrative procedures designed to protect the privacy of individuals' Protected Health Information (PHI). PHI is health information that contains identifiers, such as name, address, social security number, or other information that identifies a person.

Procedures

Designation of Privacy Officer

The Plan has designated **Hope Lindley** as the Privacy Officer. The Privacy Officer will be identified in the Plan's Notice of Privacy Practices. The Privacy Officer shall have the responsibilities described in Parts 160 and 164 of Title 45 of the Code of Federal Regulations (the "Privacy Regulations") including, but not limited to:

- Overseeing and monitoring implementation of the Plan's Privacy Policies and Procedures;
- Overseeing distribution of the Plan's Notice of Privacy Practices;
- Coordinating and participating in initial and ongoing training on the Privacy Policies and Procedures and ensuring that the appropriate members of the Plan's Workforce[1] are also trained;
- Receiving and responding to complaints about privacy matters; and
- Responding to questions about the Plan's Notice of Privacy Practices and the Privacy Policies and Procedures.

Privacy Training

The Plan shall train all members of the **Plan's Workforce** on its Privacy Policies and Procedures as necessary to carry out their functions for the Plan.

- Timing of Privacy Training
  - Individuals joining the Plan's Workforce, privacy training shall occur within a reasonable period of time after the person joins the Plan's Workforce.
  - In the event there is a material change to the policies and procedures, each member of the Workforce affected by that change shall receive privacy training within a reasonable period of time after the material change becomes effective.
  - Each member of the Plan's Workforce shall retrain every three years or upon discovery of a HIPAA violation by that member.
  - **Each member of the Plan's Workforce shall sign an acknowledgment certifying that he/she has received training and has read these Privacy Policies and Procedures.**
- Optional Training for Others

[1] The Plan's Workforce refers to those individuals who require access to Protected Health Information in order to perform plan administration functions for the Plan and are under the direct control of the Plan.

In addition to the training of the Plan's Workforce, the Plan may within its sole discretion, offer similar training to other employees who do not perform plan administration functions. For example, IT personnel may have only incidental access to PHI and are not required under HIPAA to participate in privacy training. The Privacy Officer, however, may decide that IT would benefit from HIPAA privacy training to assist the Privacy Officer in creating technical safeguards to protect the privacy of PHI.

Safeguards

The Plan will have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI. These safeguards will include the following:

- Any PHI received or stored electronically shall be saved in files with restricted access, such as department-specific network drives. Computers containing accessible PHI must have auto log off, be logged off or locked when not attended.

Confidentiality Statement

HIPAA requires appropriate administrative, technical and physical safeguards to protect the privacy of Protected Health Information (PHI).

- A confidentiality statement should be included on any e-mail that contains PHI (any documents/attachments with PHI should also be password protected). A confidentiality statement should be included on the coversheet for any fax transmission containing PHI.
- Facsimile transmissions (fax) should be sent with a cover page that includes a confidentiality statement and does not contain PHI. The fax shall not be left unattended. Before sending any fax that contains PHI, reasonable steps shall be taken to ensure that it reaches the intended recipient.

  The following statement should be used:

  This communication is privileged and contains privileged and confidential information intended only for the persons to whom it is addressed. Any other distribution, copying or disclosure is strictly prohibited. If you have received this message in error, please immediately notify the sender and destroy the original message and all copies.

- You can set up your email to have the confidentiality statement automatically added to all outgoing e-mail, or only to emails with PHI. If you currently use another confidentiality statement, please forward it to the Corporate Benefits Manager for approval related to HIPAA/PHI. If you have questions regarding how to add the statement to all out-going email contact your IT department.
- Files containing PHI may not be left unattended. It should not remain open on an individual's desk or in an individual's office when the individual is not present for extended periods (e.g., extended meetings or overnight).
- PHI should be stored in a secure location, accessible only by Plan personnel who are authorized to access it for a legitimate purpose. Where practical, PHI shall be kept in locked files or file rooms when not being used by an authorized individual.
- PHI shall not be copied except where necessary for a legitimate purpose.
- Unopened mail reasonably believed to contain PHI that is not addressed to an authorized individual shall be directed unopened to either the Privacy Officer or his or her designee.

  Mail found to contain PHI that is opened by someone other than an authorized individual, should be immediately resealed and forwarded to either the Privacy Officer or an authorized individual.

Breach Notification

Pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), adopted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), the Plan must notify the individual without unreasonable delay and in no case later than 60 days of discovering a breach of unsecured Protected Health Information.

A breach is considered discovered as of the first day on which the breach is known by the Covered Entity or Plan, the Business Associate, or Vendor.

If law enforcement determines that a notification, notice or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under 45 CFR § 164.528(a)(2).

The Covered Entity or Plan shall maintain all documentation related to the breach for a minimum of six (6) years.

Breach Notification Procedure

Unauthorized access to, use or disclosure of or improper disposal of PHI is presumed a breach. Additionally, violation of the minimum necessary standard requirement is also presumed a breach. Following discovery of a breach, a four-factor risk assessment shall be performed to gauge the level of compromise to the security or privacy of the PHI. This assessment will consider the nature and extent of PHI involved, the identity of the unauthorized user or recipient, whether PHI was actually acquired or viewed and the extent to which risk to PHI was mitigated. Documentation of this analysis and the proof of the findings shall be maintained. Breach notification is required unless the risk assessment demonstrates a low probability that the PHI has been compromised. The requirements outlined in the HITECH Breach Notification Procedure must be followed. Limited Data Sets (except those that exclude zip code and date of birth) are subject to the breach notification reporting requirements.

Patient Notification

- After a complete investigation, no later than 60 days from breach discovery, the Plan shall provide written notice to the individual or:
  - If the individual is deceased, the next of kin or personal representative.
  - If the individual is incapacitated/incompetent, the personal representative.
  - If the individual is a minor, the parent or guardian.
- Written notification shall be in plain language at an appropriate reading level with clear syntax and language with no extraneous materials. Americans with Disabilities Act (ADA) and Limited English Proficiency (LEP) requirements must be met.
- Written notification shall be sent to the last known address of the individual or next of kin, or if specified by the individual, by encrypted electronic mail. The template letter in the HITECH Breach Notification Procedure shall be used when sending written notification to an individual, personal representative, or next of kin.
- In the case where there is insufficient or out-of-date contact information:
  - For less than ten (10) individuals that precludes direct written notification to the individual, a substitute form of notice shall be provided such as a telephone call.
  - In the case that there are ten (10) or more individuals for which there is insufficient or out of date contact information and contact information is not obtained, the Plan must:
    - Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
    - Provide notice in major print or broadcast media in the geographic area where a patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice

- If the Plan determines the individual should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the Plan may, in addition to providing notice as outlined in the second, third and fourth bullets above, contact the individual by telephone or other means, as appropriate.

Media Notification

In the case where a single breach event affected more than 500 residents of the same State or jurisdiction, notice shall be provided to prominent media outlets. A jurisdiction is defined as a geographic area smaller than a state (e.g., city, county). For example, if a single breach event affects 200 patients in Florida and 400 patients in Texas, a notice to the media is not required because there were not more than 500 patients in the same State or jurisdiction affected. However, if a single breach event affects 500 patients in Florida and 500 in Texas, a media notice is required in both Florida and Texas.

HHS Notification

Notice must be provided by the Plan without unreasonable delay and in no case later than 60 days from the breach discovery to the Secretary of the Department of Health and Human Services (HHS) if a single breach event was with respect to 500 or more individuals regardless of the State or jurisdiction. You must use the **electronic form available on the HHS website** when notifying HHS of breaches involving 500 or more individuals.

If a breach is with respect to less than 500 individuals, the Plan must use the **electronic form available on the HHS website** and submit to HHS no later than 60 days after the end of the calendar year.

Facilities must maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. The log must be submitted to the corporate office no later than 60 days after the end of the calendar year. Submission to HHS shall be made annually.

Content of Notification

Regardless of the method by which the notice is provided to individuals, notice of the breach must include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured PHI that were involved in the breach, such as full name, Social Security Number, date of birth, home address, account number, diagnosis code or disability code. Only the generic type of PHI should be listed in the notice (i.e., date of birth rather than the patient's actual birth date).
- The steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

Complaint Process

The Plan will identify its complaint process in its Notice of Privacy Practices and will comply with that process. The Compliant Officer will document any complaints it receives and the resolution of those complaints.

Complaint to the Plan

- The Plan has designated the **Hope Lindley** to also be the Plan's Complaint Officer.
- The Plan shall communicate in its Notice of Privacy Practices to the participants and covered beneficiaries their rights to file a complaint with the Complaint Officer as provided under 45 C.F.R. § 164.530(d).
- The Complaint Officer shall upon request provide a copy of the complaint form to the requesting participant or covered beneficiary.
- The Complaint Officer shall thoroughly investigate all complaints filed and take the appropriate action to resolve each complaint.

Complaint to the Secretary of Health and Human Services

- Any person who believes that the Plan is not complying with the privacy standards of the Privacy Regulations may file a complaint with the Secretary of the U.S. Department of Health and Human Services.
- Corporate benefits shall be notified if a copy of a complaint from the Secretary of the U.S. Department of Health and Human Services is received by the Plan.

Sanctions

In the event that any member of the Plan's Workforce fails to comply with any of these Privacy Policies and Procedures, the individual(s) shall be subject to one or more of the following sanctions, as appropriate:

- Informal counseling concerning obligations under the Plan's HIPAA Privacy Policies and Procedures;
- Retraining concerning the Plan's HIPAA Privacy Policies and Procedures;
- Formal counseling by the individual's supervisor and/or Privacy Officer;
- Formal counseling by the individual's supervisor and/or Privacy Officer with a record in the individual's personnel file; and/or
- Removal of the privilege of receiving PHI on behalf of the Plan.

Mitigation

If the Plan learns of a harm caused by an improper use or disclosure of the Plan's PHI, the Plan will mitigate (i.e., alleviate or lessen) the harm, to the extent it is practicable to do so. This procedure applies to improper uses and disclosures by the Plan's employees, others working under the Plan's direct control, and any Business Associates of the Plan.

In an effort to mitigate the harmful effect, the Plan shall take reasonable steps to stop any further disclosure based on:

- Its knowledge of where the information has been disclosed;
- How the PHI might be used to cause harm to the person who is the subject of the PHI; and
- What steps will actually have a mitigating effect on the specific situation.

A reasonable step would include contacting the recipient of the improper disclosure and advising them not to use or further disclose the information.

No Waiver of Rights or Conditioning of Plan Benefits

The Plan will not require individuals to waive their rights under the Plan's Privacy Policies and Procedures or the federal Privacy Regulations as a condition of enrollment in the health plan or eligibility for benefits.

No Intimidation or Retaliation

The Plan will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or entity that opposes a Plan privacy practice, files a complaint regarding the Plan's privacy practices, or participates in an investigation or other review of the Plan's privacy practices.

The Plan also will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who chooses to exercise his or her right to request additional privacy protections, access, amendment/revision, or accounting.

Notice of Privacy Practices

Creation of Notice of Privacy Practices

The Plan will create and maintain a current Notice of Privacy Practices ("Notice") that describes the ways in which the Plan will use and disclose individuals' PHI. The Plan will ensure that it acts in accordance with its current Notice.

Distribution of Notice of Privacy Practices

- HIPAA Privacy Practices were effective on the aforementioned effective date.
- The Plan's Notice may be delivered personally, by mail, or by e-mail. However, it may be provided by e-mail only if:
  - The individual has currently agreed to receive the Notice electronically;
  - The Plan has not received a warning of an attempted electronic delivery failure; and
  - The individual is provided a paper copy upon request.
- If the Plan maintains a web site that provides information about the Plan's benefits, the Plan will prominently post its Notice on the web site. The posting shall not substitute for delivery of the Notice as described above.
- The Plan shall document all methods used for distribution of the Notice.

Periodic Reminder of Notice of Privacy Practice's Availability

At least **once every three years,** the Plan must notify plan participants that the Notice is available and the process to request a copy.

Updating Notice of Privacy Practices

The Plan will promptly revise its Notice whenever there is a material change to the uses or disclosures, the individual's rights, the Plan's duties or other privacy practices stated in the Notice. The Plan must also ensure that its Notice is changed to reflect any changes in law. Updated Notices will be distributed within 60 days of a material revision. If the Plan posts the Notice on its website or intranet, the revised Notice will be posted by the effective date of the material change and will provide information on how to obtain the revised notice in its annual mailing to individuals covered by the plan.

Distribution of Changes to Notice of Privacy Practices

If any change to the Plan's Privacy Policies and Procedures materially affects the provisions of the Plan's Notice of Privacy Practices, the Plan must promptly revise the Notice and distribute it within 60 days of its effective date. However, the Plan may not implement any such change to the Privacy Policies and Procedures prior to the effective date of the revised Notice except where the change is required by law.

Effect of Change on Previously Received PHI

A change to the Plan's Notice of Privacy Practices may apply retroactively if the Plan has included a provision in its Notice that reserves a right to make retroactive change. If the Plan's Notice does not include such a statement, changes to the Plan's Notice will apply only to Protected Health Information that is created or collected after the effective date of the revision.

Business Associates

A business associate in service of the Plan creates, receives, maintains, or transmits PHI for a function or activity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, repricing, administration of a self-funded plan, and disposal of PHI. Additionally, a business associate provides, in the capacity of a member of the workforce, legal, actuarial, accounting, consulting, data aggregation, management, administration accreditation or financial services.

- Business associates include:
  - A health Information Organization, E-prescribing Gateway or other person that provides data transmission services with respect to PHI to the Plan and that require routine access to PHI;
  - A person that offers a personal health record to one or more individuals on behalf of the Plan;
  - A subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate.
- A business associate does not include:
  - A health care provider, with respect to disclosures by the Plan to the provider concerning treatment of the individual;
  - A plan sponsor with respect to disclosures by a group health plan to the plan sponsor as required in § 164.504(f);
  - A government agency with respect to determining eligibility for or enrollment in a government plan that provides public benefits and is administered by another government agency or is collecting information to the extent activities are authorized by the law.

A business associate may permit a business associate that is a subcontractor to create, receive, maintain or transmit ePHI on its behalf only if the business associate obtains written satisfactory assurance that the subcontractor appropriately safeguards the information by entering into a contract that complies with the HIPAA Privacy and Security Rules. The contractor with the subcontractor shall be in the same manner as such requirements placed upon the business associates.

- The subcontractor will report to the business associate any security incident, including breaches of unsecured PHI.
- The business associate will report to the Plan and/or individuals affected by any incidents including breaches.

Record Retention and Documentation

The Plan will retain documentation of its compliance with its Notice of Privacy Practices, its Policies and Procedures, and with the Privacy Regulations. The Plan will maintain this documentation for 6 years from the date of a document's creation or the last date a document was in effect, whichever is later.

- The Plan shall maintain the following documents in written or electronic form:
  - The Plan's Privacy Policies and Procedures;
  - Any communication required by the Privacy Regulations to be in writing; and
  - Records of any action, activity, or designation required by the Privacy Regulations to be documented.
- Examples of documents that must be retained in written or electronic form:
  - Plan Privacy Policies and Procedures, including any changes;
  - Plan documents;
  - Signed authorizations;
  - Privacy Notices to individuals;
  - Designated Record Sets (see Section V. Definitions) that are subject to inspection and copying by an individual, where applicable;
  - Documentation of any requests made by an individual exercising his or her individual rights and the action taken, where applicable;
  - Complaints by individuals and the outcomes of the complaints, where applicable;
  - Records of sanctions imposed on the Plan's Workforce for violation of these Privacy Policies and Procedures;
  - Record of the Plan's action with respect to its discovery of a violation of a Business Associate contract;
  - Breach of unsecured PHI policies and procedures;
  - Accounting of Disclosure Logs, where applicable; and,
  - Business Associate contracts.

Destruction of Documents Containing PHI

When documents (whether written or electronic) containing PHI are destroyed, they must be destroyed in a manner that will reasonably prevent the reconstruction of the PHI (e.g., shredding).

USES AND DISCLOSURES OF PHI

Policy

The Plan must only use and disclose Protected Health Information in accordance with its Policies and Procedures, its Notice of Privacy Practices, and all relevant Federal and State laws.

Procedures

De-identified Information

The Plan may freely use or disclose "de-identified" information. Information is presumed "de-identified" if the following eighteen identifiers are removed:

- Names,
- All geographic subdivisions smaller than a State, except for the initial 3 digits of a zip code,

- 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
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs
- Internet protocol
- Addresses
- Biometric identifiers, including finger and voiceprints
- Full face photos or comparable images, and any other unique identifying number, characteristic or code.

De-identified information is not considered to be PHI.

Minimum Necessary

The Plan must use and disclose only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure. This minimum necessary requirement, however, shall not apply to the following:

- Disclosures to or requests by a health care provider for Treatment;
- Uses or disclosures to the individual who is the subject of the PHI;
- Uses or disclosures made pursuant to an Authorization;
- Disclosures made to the Secretary of Health and Human Services;
- Uses or disclosures required by law; and
- Use or disclosures required for monitoring compliance with the Privacy Regulations.

Implementing the Plan's Minimum Necessary Obligations

- In order to fulfill its minimum necessary obligations, the Plan shall:
  - Identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties;
  - Identify the categories of PHI to which access is needed and any conditions appropriate to the access;
  - Make reasonable efforts to limit the access of the persons to PHI consistent with the needed access and appropriate conditions;
  - For routine and recurring situations, establish protocols for what constitutes minimum necessary uses and disclosures; and
  - For non-routine and non-recurring situations, develop criteria designed to limit PHI disclosure to that reasonably necessary to accomplish the purpose of the request. Review requests for disclosure on an individual basis in accordance with the criteria.

Permitted Use and Disclosure Without an Authorization

The Plan may use or disclose PHI without an Authorization as indicated below.

To the Individual

- The Plan may use or disclose PHI to the individual who is the subject of the PHI (or his or her Personal Representative – see Section V. Definitions – "Personal Representative").

For the Plan's Treatment, Payment and Health Care Operations

- The Plan may use or disclose an individual's PHI for its own Treatment, Payment and Health Care Operations (including disclosure to its Business Associate or Plan Sponsor where otherwise permitted).

Treatment

- The Plan may disclose an individual's PHI to aid a health care provider's Treatment of the individual. For example, the Plan may provide a treating physician with the name of another treating provider to obtain records or information needed for treatment.

Payment

- The Plan may use or disclose an individual's PHI to a healthcare provider or Business Associate for Payment purposes. For example, the Plan may disclose PHI to another Covered Entity for purposes of coordination of benefits or to a stop loss or reinsurance carrier for Payment.

Health Care Operations

- The Plan may use or disclose an individual's PHI to another Covered Entity (or its Business Associate or Plan Sponsor where otherwise permitted) for Health Care Operations purposes, such as quality assessment and fraud investigation.

To Persons Involved in the Individual's Health Care

- The Plan at its own discretion based on the best interest of the individual may disclose to a family member, other relative, a close personal friend, or other person identified by the individual, PHI that is directly relevant to that person's involvement with the individual's condition, location or death.
- If the individual is deceased, the Plan may disclose to a family member or other persons identified as involved in the individual's care or payment for health care prior to the individual's death any PHI relevant to such person's involvement unless doing so is inconsistent with any prior expressed preference of the individual. Otherwise, disclosures without authorization are only permitted fifty (50) years after the individual's death.

Disaster Relief

- The Plan may use or disclose PHI to an entity authorized by law to assist in disaster relief efforts provided that the Plan, in the exercise of its professional judgment, determines that giving an individual the opportunity to object to the disclosure beforehand would interfere with the ability to respond to the emergency.

Uses and Disclosures Required by Law

- The Plan may use or disclose PHI to the extent that it is required by law and the use or disclosure complies with and is limited to the relevant requirements of the law.

Public Health Activities

- The Plan may use or disclose PHI for public health activities authorized by law.

Health Oversight Activities

- The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, civil, administrative, or criminal investigations, inspections, licensure or disciplinary actions, civil, administrative or criminal proceedings or actions, or other activities necessary for appropriate oversight

Judicial and Administrative Proceedings

- The Plan may disclose PHI in the course of any judicial or administrative proceeding under one of the following circumstances:
  - In response to an order of a court (or administrative tribunal), provided that the Plan discloses only the PHI expressly authorized by the order; or
  - In certain circumstances, in response to a subpoena, discovery request or other lawful process

Law Enforcement Purposes

- Under certain circumstances, the Plan may disclose to law enforcement officials PHI that the Plan believes in good faith should be disclosed for law enforcement purposes.

Serious Threat to Health or Safety

- The Plan may use or disclose PHI consistent with applicable law and standards of ethical conduct if it in good faith believes that the use or disclosure is necessary to lessen or prevent a serious threat to the health or safety of an individual or the public.

Workers Compensation

- The Plan may disclose PHI as authorized by and to the extent necessary to comply with workers' compensation or similar laws.

Business Associates

- The Plan may disclose PHI to its Business Associates for a permitted purpose provided that there is an agreement with the Business Associate that meets the requirements of 45 C.F.R. § 164.502(e).

Plan Sponsors

- The Plan may disclose PHI to the Plan Sponsor for a permitted purpose provided that the Plan language is amended to comply with 45 C.F.R. § 164.504(f) of the Privacy Regulations, the Plan Sponsor certifies that the amendment/revisions have been made as described in that section, and the Plan complies with the terms of the amendment/revision.

Limited Data Set Recipient (where applicable)

- The Plan may disclose to a Limited Data Set Recipient PHI consisting of a Limited Data Set if the Plan and the recipient enter into a Limited Data Set Agreement. Unlike de-identified information, the limited data set can include certain identifiers, including: admission, discharge, and service dates; date of death; age; and five-digit zip code.

Disclosure to the Secretary Of Health and Human Services

- The Plan shall disclose PHI to the Secretary of Health and Human Services when required by the Secretary to investigate or determine the Plan's compliance with the Privacy Regulations.

School

A school is permitted to disclose information about a student or prospective student of the school if:

- The PHI disclosed is limited to proof of immunization
- The school is required by law to have such proof prior to admitting a student; and
- The Plan obtains and documents the agreement to disclosure from a parent, guardian, or other person acting in loco parentis, or by the individual if an adult or emancipated minor.

Fundraising

The Plan may use or disclose to a business associate or an institutionally related foundation, the following PHI for purposes of raising funds for its own benefit, without authorization:

- Demographic information relating to an individual's address, name, contact information, age, gender and date of birth;
- Dates of health care provided;
- Treating physician;
- Outcome information; and,
- Health insurance status.

The Plan may not use or disclose PHI for fundraising for purposes other than those listed herein and a statement of such practice will be in the Notice of Privacy Practices should such use and disclosure be necessary.

With each fundraising communication made to an individual pursuant to this section, the Plan must provide the individual with a clear and conspicuous opportunity to elect not to receive further fundraising communications. The method to elect not to receive such communications shall not be unduly burdensome or more than a nominal cost. The Plan shall not condition treatment or payment on the individual's choice with respect to fundraising communications

Underwriting

- The Plan may disclose PHI for underwriting and related purposes.
- Use and disclosure of genetic information for underwriting purposes, excluding long-term care policies, shall not be used or disclosed for underwriting purposes including: determination of eligibility, determination of benefits under the plan, coverage deductibles or cost-sharing in return for completion of a health risk assessment or participation in a wellness program.
- Underwriting purposes include: the computation of premium or contribution amounts; application of any preexisting condition exclusions; and other activities related to creation, renewal or replacement of a contract of health insurance.
- Underwriting purposes does not include determination of medical appropriateness where the individual seeks a benefit under the plan.

Incidental Use or Disclosure

- The Plan may use or disclose PHI in a manner incidental to a use or disclosure that is permitted or required by the Privacy Regulations provided that the Plan has complied with:
  - The minimum necessary requirements; and
  - The safeguard requirements.

Use or Disclosure with an Authorization

Unless otherwise permitted by these Privacy Policies and Procedures, the Privacy Regulations, or applicable federal, state, or local law, the Plan may only use or disclose an individual's PHI with the individual's valid Authorization.

- The Plan must document and retain any signed Authorization as required for a period of **six (6) years** following its expiration date.
- The Plan must provide the individual with a copy of the signed Authorization.
- An individual may revoke an Authorization at any time in writing, except that the revocation shall not be effective if:
  - The Plan has already taken action based on the Authorization,
  - The Authorization was obtained as a condition of obtaining insurance coverage, when other law provides the insurer with the right to contest a claim under the policy or the policy itself.

    An example would be when a life insurer obtains the individual's authorization for the use or disclosure of PHI to determine eligibility or premiums under the policy. The individual does not have the right to revoke the authorization during any period of time in which the life insurer can contest a claim for benefits under the policy in accordance with state law.

Verifying Authority of Party Requesting Disclosure

General Rule

- The Plan shall comply with authority and identity verification requirements prior to making any disclosure of PHI. In order to comply with the verification of authority requirements, the Plan shall:
  - Verify the identity and the authority of a person requesting PHI (if the identity or authority of the person is not known); and
  - Obtain any documentation or statements from the person requesting the PHI when the documentation or statement is required by HIPAA or other applicable law.

Verification of Identity and Authority

- If the identity or authority of a person requesting disclosure of PHI is not known to the Plan:
  - The individual must provide a written statement to the Plan (generally on their company letterhead). The statement must describe the legal authority for requesting the disclosure and describe the authority under which the individual is acting.
  - Other similar written evidence may be accepted, within the sole discretion of the Privacy Officer that confirms the individual's identity and authority to make the request.
  - The Plan shall review a valid power of attorney, court order or similar legal documentation that demonstrates the Personal Representative has the authority to request the PHI.

Individual Rights

Policy

In addition to protection of health information, the Privacy Regulations create individual rights, including:

- The right to a written Notice of Privacy Practices explaining the Covered Entity's duties with respect to PHI, the uses and disclosures it may make or be required to make, and the individual's rights;
- The right to review and obtain a copy of their PHI, where such exists;

- The right to request restrictions on certain uses or disclosures of PHI for Treatment, Payment or Health Care Operations where concerning a service already paid for;
- The right to request receipt of PHI by alternative means or at alternative locations to protect confidentiality;
- The right to request amendment/revisions of PHI;
- The right to an accounting of certain disclosures, where applicable of their PHI;
- The right to receive notification, without unreasonable delay, by first-class mail of breaches involving your unsecured PHI.
- Right to not have PHI sold for remuneration unless for public health, research purposes, treatment, payment or for a sale or merger or consolidation of the Plan.

Procedures

Requests to Review/Access and Obtain PHI

General Policy

In most circumstances, an individual has the right to inspect and copy or have access to all PHI about the individual for as long as the information is maintained by the Plan. For denials, under certain circumstances, the Plan must provide the individual with the opportunity to have the denial reviewed. Under other circumstances, the Plan may deny the individual's request without the opportunity for further review.

- An individual may request access to inspect and obtain a copy of his or her PHI that is maintained in the Plan's records.
- The Plan shall not be obligated to comply with the request unless it is made in writing.
- If the Plan does not maintain the PHI that is requested, the Plan shall inform the individual in writing that the records do not exist. If the Plan knows where the PHI is maintained, the Plan shall instruct the individual in writing where to send his or her request.
- If an individual's request for access directs the covered entity to transmit the copy of PHI to another person designated by the individual, the Plan will provide the copy to the person designated. The individual's request must be in writing and signed by the individual clearly identifying the designated recipient and where to send the copy of PHI.

Form of Access

The Plan must provide the individual with access to PHI in the form or format requested by the individual if it is readily producible in such form or format. If it is not, the Plan may produce a readable hard copy. If the PHI is maintained in one or more designated record sets electronically and the individual requests an electronic copy, the Plan must provide the individual with access to the PHI in electronic form and format if readily producible; or, if not, in a readable electronic form and format as agreed to between the parties.

Time to Respond to Request

- The Plan shall respond to the request no later than thirty (30) days for information that is maintained or accessible on-site and sixty (60) days for information that is off-site.
- If the Plan cannot render a decision within the time period, the Plan must provide the individual with a written statement to extend the time for response up to an additional thirty (30) days.

Request is Granted

- If the Plan grants the individual's request for access, the Plan must:
  - Notify the individual in writing at the address provided by the individual;

- Identify the information requested and indicate the steps the individual must take to fulfill the request;
- Identify if a reasonable cost-based fee for copying will apply;
- Indicate the days of the week and hours during which the information is available, if the individual will inspect the records on-site.

Request is Denied

- If the Plan denies the individual's request for access to PHI, the Plan must:
  - To the extent possible, give the individual access to any other PHI to which it has not denied access;
  - Provide a written denial that includes:
    - The basis for the denial;
    - A statement of any right to have the denial reviewed, if applicable (see Denial with Right of Review);
    - A description of the Plan's complaint process.

Denial Without Right of Review/Access

- Denials are not subject to additional review if they are made for the following reasons:
  - The request is to inspect or copy psychotherapy notes.
  - The request is for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding;
  - The request is for information subject to the Clinical Laboratory Improvements Amendment of 1988 (CLIA), 42 U.S.C. § 263a, if the access would be prohibited by CLIA or exempt from CLIA.
  - If the information requested is not part of the Designated Record Set.
  - The request is for information that was obtained under a promise of confidentiality and inspection is likely to reveal the source.
  - The request is made during the duration of a research trial and the request is for information created or obtained in the course of research that includes treatment and the individual had consented to a denial of access when consenting to participate.

If the request is for information contained in records subject to the federal Privacy Act, 5 U.S.C. 552a and denial would be appropriate under that law. *Denial with Right of Review/Access*

- Denials are subject to additional review if they are made for the following reasons:
  - A licensed health care professional has determined that the requested access is reasonably likely to endanger the life or physical safety of the individual or another person.
  - The information is about another person and inspection is reasonably likely to cause substantial harm to that person.
  - The request is made by the individual's Personal Representative and a licensed health care professional has determined that the provision of access to the Personal Representative is reasonably likely to cause substantial harm to the individual or another person.

Review of Denial

Where the denial is reviewable, the review shall be made by a licensed health care professional designated by the Plan who did not participate in the original decision to deny access. The Plan shall provide or deny access in accordance with the health care professional's determination.

Time for Considering Request for Review/Access

Within 15 days of receipt of the request for review of a denial based on grounds of endangerment, the Plan will submit the individual's request to a licensed health care professional described above. The

decision will be reviewed within thirty (30) days and the Plan will notify the individual in writing within fifteen (15) days of the final decision.

Request to Restrict Use or Disclosure of PHI

An individual may request that the Plan restrict its use or disclosure of the individual's PHI beyond the scope of these Policies and Procedures by contacting the Plan's Privacy Officer.

- Such requests shall be made in writing to the Plan's Privacy Officer.
- The Plan is under no obligation to accept the restrictions other than for disclosures for the purposes of carrying out payment or health care operations and is not otherwise required by law and where services rendered are already paid in full out-of-pocket. If the Plan accepts, it is bound to honor the restrictions, to the extent it does not prevent the use and disclosure of PHI that is required by the Privacy Regulations.
- The Plan may terminate its agreement to restrictions, if:
  - The individual agrees to or requests the termination in writing;
  - The individual orally agrees to the termination and the oral agreement is documented; or
  - The Plan informs the individual that it is terminating its agreement to the restriction.

If the Plan informs the individual that it is terminating its agreement to the restriction, the termination is only effective with respect to PHI that is created or received after the Plan has informed the individual of the termination.

An individual may request to terminate restrictions on use or disclosure of PHI; however, the request may only apply to uses or disclosures made after receipt of the request for termination of restrictions.

Request to Receive Confidential Communications

An individual may request that the Plan use an alternative means for communicating PHI to protect the confidentiality of that individual's PHI.

- The request must be in writing and the individual must indicate that he or she would be endangered if the request were not granted.
- The Plan shall accommodate a reasonable request if the above criteria are met.

Requests to Amend/Revise PHI

Right to Request Amendment/revision

An individual may request that the Plan amend/revise his or her PHI in the Plan's records, at any time while the Plan maintains the information. The request shall be in writing.

Reasons for Denying Request

- The Plan may deny an individual's request for an amendment/revision for any of the following reasons:
  - The Plan did not create the information and the originator is available to make the amendment/revision;
  - The information is not part of the Plan's Designated Record Set;
  - The information would not be available for inspection by the individual as described under *Denial Without Right of Review*; or
  - The information is accurate or complete.

Time for Considering Request

- The Plan shall render a decision regarding the individual's request for an amendment/revision no later than sixty (60) days after the Plan receives the individual's written request.
- If the Plan cannot render a decision within that time period, the Plan shall provide a written statement to extend the time for response to no more than an additional thirty (30) days.

Amendment/Revision Request Granted

- If the Plan grants the individual's request for an amendment/revision, in whole or in part, the Plan must:
  - Make the appropriate amendment/revision to the PHI or record that it is the subject of the request for amendment/revision by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment/revision;
  - Notify the individual in writing that the amendment/revision is accepted;
  - Obtain the individual's identification of and agreement to have the Plan notify the relevant persons with which the amendment/revision needs to be shared;
  - Make reasonable efforts to inform and provide the amendment/revision to:
    - Persons identified by the individual as having received PHI about the individual and needing the amendment/revision; and
    - Persons, including Business Associates that the Plan knows maintain the information that is subject to the amendment/revision.

Amendment/Revision Request Denied

- If the Plan denies the individual's request for an amendment/revision of PHI, the Plan must provide the individual with a written denial that contains:
  - The basis for the denial;
  - How the individual may file a written statement of disagreement;
  - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the request for amendment/revision and the denial with any future disclosures of that PHI; and
  - How the individual may lodge a complaint.

The individual may submit a written statement to the Plan disagreeing with the denial of all or part of a requested amendment/revision. The written statement may be no longer than five (5) pages.

The Plan may, in its sole discretion, prepare a written rebuttal to the individual's statement of disagreement. Whenever the rebuttal is prepared, the Plan shall provide a copy to the individual who submitted the statement of disagreement.

Actions on Notices of Amendment/Revisions

If the Plan is informed by another entity that is subject to the Privacy Regulations of an amendment/revision to an individual's PHI and the notice is made in accordance with the Privacy Regulations, then the Plan shall amend/revise the PHI in the Designated Record Sets.

Requests for an Accounting of Disclosures of PHI

An individual may request an accounting of disclosures made by the Plan of the individual's PHI. This right extends to disclosures made for the past six years (or for a shorter time period if so requested by the individual).

Time for Considering Request

Upon receiving the request, the Plan must act within 60 days to provide an accounting, or deny the request based on one of the approved reasons for denial, or provide a written statement to extend the time for the accounting to no more than an additional thirty (30) days.

Procedure to Request an Accounting

An individual may request an accounting at any time in writing by completing the request form developed by Privacy Officer for this purpose and returning the form to the Privacy Officer.

Content of the Accounting

- For each disclosure, the Plan must account each of the following:
  - The date of the disclosure;
  - The name and address of the recipient;
  - A brief description of the information disclosed; and
  - One of the following:
    - A description of the purpose of the disclosure;
    - A copy of the individual's written authorization; or
    - A copy of the written request for disclosure.

Multiple Disclosures

The Plan may use summary information for multiple disclosures to the same recipient for the same purpose.

Denial of Request

If the Plan denies a request for an accounting, the Plan must notify the individual of the denial and inform the individual of the basis for denial. The Plan may deny an individual's request for an accounting for any of the following reasons:

- The disclosure was for the purpose of carrying out Treatment, Payment or Health Care Operations
- The disclosure was made to the individual.
- The disclosure was made in response to a valid Authorization.
- The disclosure was for national security or intelligence purposes.
- The disclosure was made to correctional institutions or law enforcement officials.
- The disclosure occurred prior to August 1, 2005.

Reasonable Fee Requirement for Subsequent Accountings

The Plan shall provide the first accounting to an individual during any twelve (12) month period without charge. For any subsequent accountings in a twelve (12) month period, the Plan may charge the individual a reasonable, cost-based fee if the Plan notifies the individual of the fee in advance and allows the individual to withdraw or modify his or her request in order to avoid or reduce the fee.

Maintenance of Log

With respect to all PHI maintained by the Plan, the Plan shall maintain a log of all the PHI's uses and disclosures as described. Such accounting shall be maintained for a period of three years.

Definitions

"**Authorization**" means written permission meeting the requirements of 45 C.F.R. § 164.508(b) from the Individual to use or disclose his or her PHI in circumstances where its use or disclose may not otherwise be permitted by the Privacy Regulations.

"**Breach**" means the unauthorized acquisition, access, use or disclosure of unsecured, unencrypted protect health information which compromises the security or privacy of such information. A breach does not include:

- Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if:
  - Such acquisition, access, or use was made in good faith and within the course and scope of authority
  - Such information is not further used or disclosed in a manner not permitted; or
- Any inadvertent disclosure by a person who is authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
- A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

"**Business Associate**" means (not Carriers / Health Plans) who on behalf of the Plan, but other than in the capacity of a member of the Plan's Workforce performs or assists in the performance of the following:

- A function or activity involving use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, care coordination, pre-certification, case management, bill audits, claim repricing, practice management or repricing;
- Underwriting premium rating or other activities related to the renewal or replacement of a contract of health insurance or health benefits or ceding a new insurance policy or reinsurance or stop loss policy;
- Conducting quality assessment and improvement activities, outcomes evaluation and population based activities on improving health or reducing health costs or other activity defined as Health Care Operations under 45 C.F.R. § 164.501 for the Plan;
- Any other function or activity regulated by the Privacy Regulations; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Plan, where the provision of the service involves a disclosure of PHI from the Plan, or from another Business Associate of the Plan, to the person.
- Notwithstanding the foregoing, another Covered Entity is not a Business Associate of the Plan to the extent it is performing a function with respect to the Plan that makes it a Covered Entity.

"Subcontractor" includes an organization or person who performs a function on behalf of the business associate and by way of that service or function has access to PHI.

"Covered Entity" includes the Plan (self-funded plans, carriers and Flexible Spending Accounts and/or Employee Assistance Programs), other health plan, a health care clearinghouse, and a health care provider who transmits any health information in electronic form.

"**Designated Record Set**" means a group of records maintained by or for the Plan that are:

- The medical records and billing records about individuals maintained by or for a health care provider;
- The enrollment, Payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
- The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity, including the Plan.

"**Health Care Operations**" means activities including the following:

- Quality assessment;
- Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, disease management, contacting health care providers and patients with information about Treatment alternatives and related functions;
- Rating providers and Plan performance, including accreditation, certification, licensing or credentialing activities;
- Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to health care claims (including stop-loss insurance and excess of loss insurance);
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Plan, including formulary development and administration, development or improvement of Payment methods or coverage policies;
- Business management and general administrative activities of the Plan, including but not limited to:
  - Management activities relating to the implementation of and compliance with HIPAA's administrative simplification requirements, or
  - Participant service, including the provision of data analyses for participants or the Plan Sponsors;
  - Resolution of internal grievances; and
  - The sale, transfer, merger, or consolidation of all or part of the Plan with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to the activity.

"**HIPAA**" means the federal Health Insurance Portability and Accountability Act of 1996.

"Genetic Information"

- Individual genetic tests;
- The genetic tests of family members of the individual;
- The manifestation of a disease or disorder in family members; or
- Any requests for or receipt of genetic services or participation in clinical research which includes genetic information.
- Includes the genetic information of a fetus carried by the individual or family member who is pregnant; and
- An embryo legally held by an individual or family member utilizing an assisted reproductive technology.
- Genetic information excludes information about sex or age of any individual.

"**Limited Data Set**" means PHI that excludes certain identifiers as described in 45 C.F.R. § 164.514(e).

"**Limited Data Set Recipient**" means one who receives PHI that qualifies as a Limited Data Set.

"**Electronic Storage Media**"

- On which data is or may be recorded electronically, including devices in computers, hard drives, and any removable/transportable digital memory medium such as magnetic tape or disk, optical disk or digital memory card.

"**Marketing**"

- Includes communications to an individual about a product or service that encourages the recipient of the communication to purchase or use the product or service, and an arrangement between the Covered Entity and another entity, under which the Covered Entity discloses PHI to the other entity, for direct or indirect remuneration, so that the other entity can make a communication about its product or service in order to encourage the recipient of that communication to purchase or use the product.

- Excludes communication made to an individual:
  - To describe a health related product or service (or Payment for the product or service) that is provided by or included in the Plan's benefits, including communications about:
    - Describing the entities participating in a health care provider network or health Plan network;
    - Replacements of or enhancements to the Plan; or
    - Health-related products or services available only to enrollees in the Plan that add value to but are not part of the Plan's benefits; or
  - For Treatment of that individual; or
  - For case management or care coordination for that individual or to direct or recommend alternative Treatments, therapies, health care providers or setting of care to the individual.

"**Organized Health Care Arrangement**" means:

- A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
- An organized system of health care in which more than one plan participates, and in which the participating covered entities:
  - Hold themselves out to the public as participating in a joint arrangement; and
  - Participate in joint activities that include at least one of the following:
    - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    - Quality assessment and improvement activities, in which Treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf;
    - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a Plan is reviewed by other participating covered entities or by a third party on their behalf for purpose of administering the sharing of financial risk.
- A group health plan and a health insurance issuer or HMO with respect to the group health plan, but only with respect to protected health information created or received by the health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in the group health plans;
- A group health plan and one or more group health plans each of which are maintained by the same Plan Sponsor; or
- The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to the group health plans, but only with respect to protected health information created or received by the health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of the group health plans.

"**Payment**" means activities undertaken by the Plan to obtain premiums or determine or fulfill its responsibility for coverage and provision of the Plan's benefits or provide reimbursement for the provision of health care that relate to an individual to whom health care is provided. A disclosure for Payment will be limited to the minimally necessary information. An Authorization is not required to permit a disclosure or use for Payment unless the disclosure involves Psychotherapy Notes. Payment activities include, but are not limited to, the following:

- Determination of eligibility, coverage and cost sharing amounts (for example, the reasonable or usual and customary cost of a service or supply, benefit Plan maximums, coinsurance, deductibles and co-payments as determined for an individual's claim);
- Coordination of benefits;
- Adjudication of health benefit claims (including appeals and other Payment disputes);
- Subrogation of health benefit claims;
- Establishing employee contributions;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;

- Billing, collection activities and related health care data processing;
- Claims management and related health care data processing, including auditing Payments, investigating and resolving Payment disputes and responding to participant inquiries about Payments;
- Obtaining Payment under a contract for reinsurance (including stop-loss and excess of loss insurance);
- Medical necessity, experimental or investigational Treatment or other coverage reviews or reviews of appropriateness of care or justification of charges (including hospital bill audits);
- Utilization review, including pre-certification, pre-authorization, concurrent review, retrospective review, care coordination or case management;
- Disclosure to consumer reporting agencies related to the collection of premiums or reimbursement (the following PHI may be disclosed for Payment purposes: name and address, date of birth, Social Security number, Payment history, account number and name and address of the provider and/or health Plan); and
- Reimbursement to the Plan.

"**Personal Representative**" means any person who has the right and authority under state law to make health care decisions on behalf of the individual, including surrogates such as a court-appointed guardian, persons with power of attorney, and others acting on behalf of an adult or emancipated minor, and parents, guardians and persons acting in loco parentis for a minor. An executor, administrator or other person who has authority under state law to act on behalf of a deceased individual or the individual's estate is also a Personal Representative.

"**Plan**" means the Company health and welfare plan including its component plans: Dental Plan, Vision Plan, Employee Assistance Program and Flexible Spending Account.

"Plan Sponsor" means the Company sponsoring the health and welfare plan as indicated on the first page.

"Plan's Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of the entity, whether or not they are paid by that entity. The Plan's Workforce is required to have access to Protected Health Information to perform their work.

"**Protected Health Information**" or "**PHI**" includes any information, including genetic information, that relates to the past, present, or future physical or mental health of an individual or to Payment for the provision of health care of an individual that was created or received by a Covered Entity and which identifies the individual or has not been de-identified as described in 45 C.F.R. §§ 164.514(a) and (b). Also identified by the term Personal Health Information and can occur in oral, written or electronic form.

"**Privacy Regulations**" means Subparts A – C of 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164.

"**Psychotherapy Notes**" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests and any summary of the following items: diagnosis, functional status, the Treatment plan, symptoms, prognosis and progress to date.

"**Summary Health Information**" means information (1) that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a Plan Sponsor has provided health benefits under a group health plan; and (2) from which the "identifiers" have been deleted, except that geographic protected health information need only be aggregated to a five digit zip code.

"**Treatment**" means the provision, coordination or management of health care and related services by one or more health care provider(s). Treatment includes:

- The coordination or management of health care by a health care provider and a third party;

- Consultation between health care providers about an individual patient; or the referral of a patient from one health care provider to another.

"Unsecured PHI" means protected health information that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

TO BE PLACED IN PRIVACY OFFICER'S HIPAA FILE