[INSERT COMPANY NAME]
CORPORATE POLICY & PROCEDURE MANUAL
FOR GROUP HEALTH PLAN

HIPAA PRIVACY

GENERAL PRIVACY POLICY

A group health plan is required by Federal law to maintain the privacy of Protected Health Information (PHI) and provide certain rights to individuals in relation to their PHI. The plan is required to abide by the terms of our Notice of Privacy Practices and the Federal law. The plan will not discriminate against or take retaliatory action against an individual for exercising their rights under HIPAA or for filing a complaint regarding our privacy practices. The plan will not condition payment of benefits, enrollment or eligibility on an individual waiving their rights under HIPAA. To the extent practical, the plan will relieve any harmful affect resulting from our use or disclosure of PHI in a way that violates Federal law or our privacy policies.

PHI is information, including demographic information, that may identify the individual and that relates to health care services provided to that individual, the payment of health care services provided to that individual, or the individual's physical or mental health or condition, in the past, present or future.

All requests for and disclosures of PHI will be limited to the minimum necessary information to complete the job for which the information is being requested or disclosed.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

The plan will not use or disclose PHI without a signed HIPAA Authorization from the individual approving the use or disclosure, except for the following purposes allowed by Federal law. Please note that other forms of authority or authorization may be required in some cases.

- ❑ Payment. The collecting of premiums and paying of claims.
- ❑ Health Care Operations. The basic business functions necessary to operate a group health plan.
- ❑ Disclosures to the covered individual.
- ❑ Disclosures to a personal representative designated by the individual to receive PHI or a personal representative designated by law, or the representative of the estate of a deceased individual.
- ❑ Disclosures to the Secretary of Health and Human Services (HHS) or any employee of HHS as part of an investigation to determine our compliance with the HIPAA Privacy Rules.
- ❑ Disclosures to a Business Associate as part of a contracted agreement to perform services for the plan.
- ❑ Disclosures to a health oversight agency, such as the Department of Labor (DOL), the Internal Revenue Service (IRS) and the Insurance Commissioner's Office.
- ❑ In response to a court order, subpoena, discovery request or other lawful judicial or administrative proceeding.
- ❑ As required for law enforcement purposes.
- ❑ As required to comply with Workers' Compensation or other similar programs established by law.
- ❑ Disclosures to the Plan Sponsor, as necessary to carry out administrative functions of the plan.
- ❑ In providing information about treatment alternatives and health services that may be of interest to the individual as a result of a specific condition that the plan is case managing.

INDIVIDUAL RIGHTS

The plan is required to provide the following rights to individuals in relation to their PHI:

- ❑ The right to request restrictions on uses and disclosures of their PHI.
- ❑ The right to receive confidential communications of their PHI.
- ❑ The right to access, view or obtain a copy of their PHI.
- ❑ The right to amend their PHI if it is incorrect.
- ❑ The right to receive an accounting of certain types of disclosures of their PHI.

HIPAA PRIVACY DESIGNATIONS

The following designations have been made, as required by the HIPAA Privacy Rule.

Privacy Officer: _____

Office to Receive Privacy Complaints: _____

Office to Receive Privacy Notice Inquiries: _____

Office to Handle Requests for Restriction of Uses/Disclosures, Access to PHI, Amendment of PHI, Accounting of PHI Disclosures: _____

MINIMUM NECESSARY RULE

WHAT IS IT?

HIPAA requires that all disclosures and requests for disclosure of protected health information (PHI) be limited to the minimum amount of PHI necessary to complete the function or task for which the PHI is being requested or disclosed.

POLICY

All uses and disclosures of PHI, internally and externally, will be limited to the minimum necessary amount of PHI to complete the task. When possible and appropriate, de-identified data will be used in place of PHI.

Access to all systems containing PHI, electronic and paper, will be limited according to job-based user profiles and the need for that user to have access to PHI.

Standard protocols will be developed for all standard or recurring external disclosures of PHI. Protocols will include tracking and verification that the party has any necessary agreements for access (Business Associate Agreement) signed and on file prior to making the disclosure.

All non-standard or unique requests for external disclosure of PHI will be reviewed by the Privacy Officer to determine if disclosure is appropriate and if any contractual agreements are necessary prior to making the disclosure.

PROCEDURE

Standard/Recurring Disclosures

Although some requests, as noted below, can be assumed to comply with the minimum necessary rule because they are requested from a government agency, Covered Entity (provider, group/insurance company) or Business Associate, judgement should be used in providing information that clearly does not seem necessary or appropriate.

1. **Agents** can be given detailed eligibility, claim and billing information provided they have a signed Business Associate Agreement on file. Requests from the agent can be assumed to be for the minimum necessary information. Without a signed agreement on file, the agent will not be provided any information, whether summary or detail.

2. **Reinsurance/Stop-Loss Carriers** can be given detailed eligibility and claim information. Signed agreements are not required, per Health and Human Services (HHS), because the carrier is acting as a covered entity on their own behalf and is not a Business Associate of the group health plan. Requests from another covered entity can be assumed to be for the minimum necessary information.

3. **Business Associates (e.g. UR Companies, PBM's, Networks)**. Disclosures of detailed claim and eligibility information can be provided between Business Associates that are contracted with the group health plan. Requests from a contracted Business Associate of a plan can be assumed to be for the minimum necessary information.

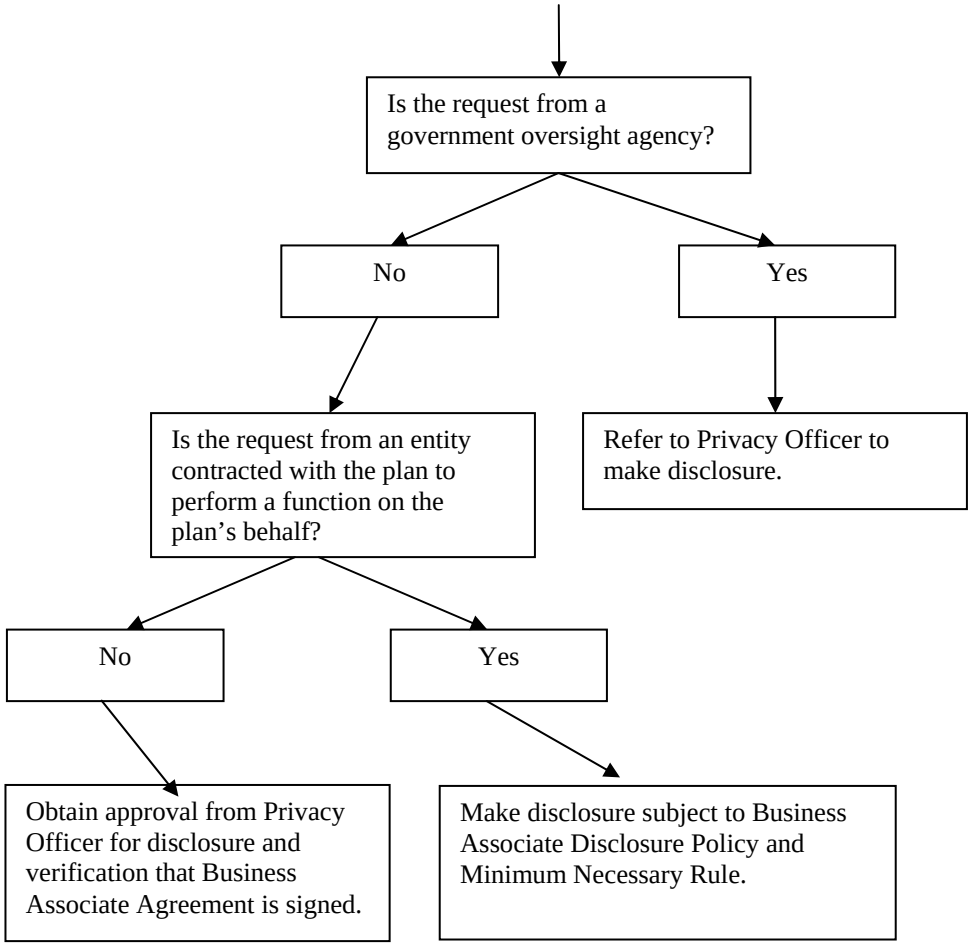
4. **Providers**. Disclosure can be made of eligibility and claim information in relation to a claim from a provider or a service the provider will be performing. Requests from a provider can be assumed to be for the minimum necessary information.

5. **OCI/DOL/Other Regulatory Agencies**. Disclosure of eligibility and claim information can be made to oversight agencies as required by law or as requested by the agency. Requests can be assumed to be for the minimum necessary information.

Unique/Non-recurring Disclosures

The Privacy Officer will make decisions concerning unique or non-recurring requests to disclose PHI based on the following Decision Rules model.

DECISION RULES FOR UNIQUE OR NON-RECURRING REQUEST TO DISCLOSE PROTECTED HEALTH INFORMATION



IDENTITY/AUTHORITY VERIFICATION

WHAT IS IT?

HIPAA requires that prior to disclosing protected health information (PHI) the identity of the person requesting the PHI and that person's authority to have access to the PHI be verified.

POLICY

Disclosures of PHI will not be made in any format – verbal, written or electronic (email or fax) – without first verifying the identity of the person making the request and their authority to access the information. If a signed authorization is required to make the disclosure, a copy of the signed authorization must be obtained prior to making the disclosure.

PROCEDURE

If the identity and authority of the person who is requesting PHI has been verified as indicated below, the release of PHI to the person is allowed. For requests to discuss PHI with a third party that does not already have authority (e.g., requester is not an agent, relative, another group employee, or management staff), verbal permission must be received from the individual whose PHI is the subject of the request (subject individual). The identity and authority of the subject individual must be verified as described below and the subject individual must be present (in person or on the telephone) during the discussion.

PHI will only be sent to the address, fax or email listed in company records. If the email address or fax number is not documented in our records or the individual whose identity and authority has been verified is requesting we use a different email address or fax number, the new number or address must be verified by having the individual send a fax or email from that number or address to which we will then respond with the information requested.

Verification of Identity

Identity will be verified by having the individual provide the following information, which must match the information contained in company records:

1. Subject individual/patient's name (First, Middle Initial, Last);
2. Subject individual/patient's Date of Birth;
3. Enrollee Social Security Number, and
4. If requester is not a provider, the requester's name and relationship to the subject individual/patient or, if requester is a provider, the provider name and TIN or address.

Verification of Authority

A limited amount of PHI may be disclosed when identity and authority have been verified. This includes eligibility, claim or premium payment, and plan benefit and coverage information.

With the exception of requests by an individual or their personal representative to access the individual's PHI, as described in the Policy on Requests to Access Protected Health Information, diagnosis and procedure code information, and demographic information (e.g. address, phone number, Social Security Number, and birth date) will not be disclosed, even if identity and authority have been verified.

Person Requesting PHI	**Authority to Access <u>Limited</u> PHI**
Provider	Okay.
Enrollee	Okay, unless there is a documented request to communicate the PHI by alternate means or location.
Spouse	Okay to provide an individual with his/her own PHI or the PHI of his/her adult or minor child only, unless there is a documented request to communicate the PHI by alternate means or location.
Adult Child (18 or over)	Okay to provide the adult child with his/her own PHI only.
Minor/Dependent Child (under 18)	Not allowed without a valid, signed HIPAA Authorization.
Employer/Plan Sponsor	Okay if the plan is amended regarding HIPAA Privacy. Otherwise, authorization from the subject individual is required.
Personal Representative	Okay to provide the personal representative with PHI for the person being represented only (subject individual). See procedure on Personal Representatives
Business Associate	Okay if a signed Business Associate Agreement is on file.
Attorney	Not allowed without a valid, signed HIPAA Authorization.
Custodial Parent not on the same plan as dependent child	Okay to provide the custodial parent with the dependent child's PHI only, unless there is a documented request to communicate the PHI by alternate means or location.
Health Oversight Agency	Refer the request to the Privacy Officer, who can release PHI to a Health Oversight Agency as appropriate.
Other Insurance Co. or Health Plan	Not allowed except for verification of coverage dates.
All Others	Not allowed.

DISCLOSURE TO GROUPS

POLICY

Protected health information (PHI) will not be disclosed to other parts of the employer group unless the group has provided written documentation that it has amended its plan documents to limit its uses of PHI, as required by HIPAA.

Summary health information (information that summarizes the history, expense or type of claims incurred by individuals covered by the group health plan, but does not specifically identify the individual) and information on plan enrollment and termination can be provided to the employer group.

DISCLOSURE TO BUSINESS ASSOCIATES

POLICY

Protected health information (PHI) will not be disclosed to a Business Associate unless a signed Business Associate Agreement is in place with the entity.

PROCEDURE

1. Unless already documented that a Business Associate Agreement has been signed, any request from the Business Associate to release PHI must be sent to the Privacy Officer.
2. The Privacy Officer will verify if a Business Associate Agreement has been signed by the entity.
3. If an agreement was signed by the entity, the Privacy Officer will communicate that release of PHI can be approved and set up.
4. If a signed agreement is not in place, the Privacy Officer will determine whether a Business Associate Agreement is appropriate or if the plan will not release PHI to the entity.
5. If the Privacy Officer determines that we have a relationship with the entity that requires the sharing of PHI, the Privacy Officer will send a Business Associate Agreement to the entity as appropriate for signature and will notify them that the release of PHI can be approved and set up.
6. If the Privacy Officer determines that we do not have a need to share PHI with the entity, the Privacy Officer will notify the referring individual that PHI cannot be released to the entity.
7. When the referring individual receives the notification from the Privacy Officer, the request will be handled as instructed with the entity.

PERSONAL REPRESENTATIVE

WHAT IS IT?

HIPAA requires that representatives of a subject individual be treated as if they were the subject individual when:

1. The representative has legal standing to act on behalf of the subject individual who is an adult or emancipated child.
2. The representative is the parent or guardian of the subject individual who is a minor child.
3. The representative is the executor or administrator of the deceased subject individual or the deceased subject individual's estate.

POLICY

After verifying the authority of the person to act as a personal representative, access to the subject individual's protected health information (PHI) will be provided to the personal representative to the same extent that access would be provided to the subject individual.

PROCEDURE

Verification of the representative's authority to act on behalf of the individual will be satisfied as follows.

Personal Representative of Adult or Emancipated Child

One of the following forms of authority must be provided:

1. Designation of Authorized Representative Form (DOL Claim Regulations Form).
2. Executed copy of Power of Attorney.
3. Copy of court order giving authority.

Personal Representative of Minor Child

1. Name matches parent or step-parent.
2. Guardianship papers are provided.
3. Designation of Authorized Representative Form (DOL Claim Regulations Form) is provided and signed by the parent on file.

Personal Representative of Deceased Individual

A copy of the will or court papers designating the representative as the executor or administrator.

REQUEST TO RESTRICT USES & DISCLOSURES

WHAT IS IT?

HIPAA guarantees all individuals the right to request restrictions on the manner in which their protected health information (PHI) is used and disclosed. While a group health plan is not generally required to agree to requested restrictions in how it uses and discloses PHI, it is required to allow individuals to make requests and to respond to those requests. The one request that a group health plan is required to accommodate is a request to provide PHI by an alternate means or at an alternate location.

POLICY

All requests to limit how PHI is used or disclosed, with the exception of requests to provide PHI by alternate means of communication or at an alternate location, will be declined. Requests to provide PHI by an alternate means of communication or at an alternate location will be reviewed and reasonable requests that can be accommodated will be approved, provided the request specifically indicates in writing that disclosure by normal means will be an endangerment. If the request for alternate means of communication or location cannot be accommodated, a reasonable alternative will be offered.

PROCEDURE

General Requests to Restrict Uses and Disclosures of PHI

1. All requests to limit the use or disclosure of PHI must be in writing.
2. When the written request to limit the use or disclosure of PHI is received, it is routed to the Privacy Officer for review.
3. The Privacy Officer will review the request to determine whether it is a request to provide PHI by an alternate means or location.
4. If the request is not a request to provide PHI by alternative means or location, the Privacy Officer will respond to the request, within 30 days of receipt of the request, with a completed PHI Restriction on Uses and Disclosures letter.
5. The request and response will become part of the subject individual's file and will be maintained for a period of at least 6 years.

Requests to Provide PHI by Alternate Means or Location

1. All requests to provide PHI by an alternate means or location must be in writing on the PHI Alternate Means or Location Form.
2. When the signed form is received it is routed to the Privacy Officer for review.
3. The Privacy Officer will review the form to determine whether the request clearly indicated that disclosure by normal means could be an endangerment and whether the subject individual is a minor child.
4. The Privacy Officer will respond to the request, within 30 days of receipt of the request, by completing the Health Plan Review/Reply section of the PHI Alternate Means or Location Form and sending a copy of the entire form back to the requesting individual.
5. The request and response will become part of the subject individual's file and will be maintained for a period of at least 6 years.

TEXT of PHI Restriction on Uses and Disclosures Letter

RE: Request to Restrict Use or Disclosure of Protected Health Information

Dear _____,

We have received a request to limit the manner in which your protected health information (PHI) is used.

The Health Insurance Portability and Accountability Act (HIPAA) does not require a group health plan to agree to requests to restrict its use or disclosure of PHI. We are therefore declining your request.

Sincerely,

TEXT of PHI Alternate Means or Location Form

REQUEST FOR DISCLOSURE BY ALTERNATE MEANS OR LOCATION

The Health Insurance Portability and Accountability Act (HIPAA) requires a group health plan to accommodate reasonable requests to provide protected health information (PHI) by an alternative means or at an alternative location when an individual clearly indicates that disclosure by normal means could endanger the subject individual. A request to provide all PHI relating to the individual at an alternate address designated by the individual will be considered a reasonable request. Requests received from unemancipated minors will not be accepted.

Please complete the information below and send this form to: **[INSERT YOUR COMPANY'S NAME AND ADDRESS]**.

IDENTIFICATION

Name:_____ Birth Date:_____

Enrollee #:_____ Relationship to Enrollee:_____

ENDANGERMENT

Would disclosure of your PHI by normal means endanger you? ☐ Yes ☐ No

If yes, please briefly describe the nature of endangerment:

_____

_____

ALTERNATE ADDRESS

I request that all communications of my PHI be provided to me at the following alternate address:

_____

Street Address City State Zip-Code Phone

I understand that disclosures of my PHI that are in progress on the date this request is received will not be affected by this request. I also understand that the enrollee will continue to receive notice of payments the group health plan makes for services provided to me, as required by law.

_____ _____

Signature of Patient or Patient's Authorized Representative **Date**

_____

If signature is Authorized Representative's, please indicate relationship or authority to act for individual.

HEALTH PLAN REVIEW/REPLY SECTION

This section is for use by authorized representatives of the group health plan only.

Date Received:_____

Title of Reviewer:_____ Date:_____

This request for communication of PHI by alternate means or location is being:

- ☐ Approved.
- ☐ Declined because endangerment to the individual has not been clearly stated.
- ☐ Declined because the requesting individual is a minor and does not have authority to make this request.

Provided for Informational Purposes by UMR.

AUTHORIZATION

WHAT IS IT?

An authorization is permission from the individual to use or disclose their protected health information (PHI) for a specific purpose. Under HIPAA, an authorization must contain specific provisions that have been included in the Authorization to Release Protected Health Information form.

HIPAA does not require that an authorization be obtained for the following uses and disclosures of PHI:

1. Those made in carrying out the functions of payment and health care operations, except for medical records requests for psychotherapy notes.
2. Those made to health oversight agencies, such as the DOL, IRS and OCI.
3. Those made in relation to legal hearings.

However, providers are not required to release PHI without a signed HIPAA Authorization and may request such an authorization, even if it may not be required for the indicated use or purpose.

POLICY

Enrollment in the plan, receipt of benefits, and claim payment will not be dependent on the signing of an authorization to obtain PHI. We will continue to use the standard authorization on the enrollment form for all PHI requests, except for requests to obtain psychotherapy notes. In cases that involve psychotherapy notes or where a provider requires a HIPAA Authorization, the Authorization to Release Protected Health Information form will be used.

PROCEDURE

If a HIPAA Authorization is required:

1. Section 1 will be completed on the Authorization to Release Protected Health Information form.
2. The authorization form will be sent to the claimant for signature.
3. When the signed authorization form is received, it will be attached to the request for medical records and sent to the provider. NOTE: Faxed copies of the authorization are acceptable.
4. The signed authorization will become part of the individual's file and will be maintained for a period of at least 6 years.

Other Uses for the Authorization to Release Protected Health Information Form

The authorization form may also be used to accommodate requests by the individual to disclose PHI to third parties, such as a parent or spouse.

AUTHORIZATION
TO RELEASE
PROTECTED HEALTH INFORMATION

SECTION 1 - To be completed by Person or Company requesting release of protected health information

Patient Name:_____ **Enrollee Social Security Number:**_____

Group Name: _____ **Group #:** _____

Person/Organization Requesting Information: **Person/Organization Providing Information:**

_____ _____

_____ _____

_____ _____

_____ _____

Description of Protected Health Information Requested, Including Date(s):

_____

_____

_____

_____

Description of Reason for Disclosure:

_____

_____

_____

SECTION 2 - To be completed by Individual giving authorization to release protected health information

I hereby authorize the use or disclosure of my protected health information as described below. I understand that this authorization is voluntary. I understand that the information to be released may be redisclosed by the recipient and no longer subject to the protection of the Federal Privacy Regulations.

I understand that the plan cannot make my eligibility for benefits or payment of claims dependent on the signing of this authorization.

I understand that I may revoke this authorization at any time by notifying the Requesting Person/Organization in writing that I am revoking the authorization. Such actions will not affect actions taken by the Requesting Person/Organization prior to the date they receive your written request to revoke the authorization.

I understand that this authorization will expire one year from the date of signature.

_____ _____

Signature of Patient or Patient's Authorized Representative **Date**

_____

If signature is Authorized Representative's, please indicate relationship or authority to act for individual.

REQUEST TO ACCESS PROTECTED HEALTH INFORMATION

WHAT IS IT?

HIPAA guarantees all individuals the right to obtain a copy of or review their protected health information (PHI), as maintained in a designated record set, for as long as the information is maintained.

POLICY

Upon written request, the individual will be given access to inspect or obtain a copy of their PHI. Records subject to inspection include:

1. Claim records.
2. Enrollment records.
3. Underwriting files, including medical records obtained.
4. Case management and utilization review/precertification files.

Access will only be denied if it is determined that the requested information:

1. Is not in our files.
2. Is psychotherapy notes.
3. Was compiled for use in a legal proceeding.
4. Is subject to the Privacy Act (5 USC 552a) dealing with information held by or on behalf of a federal government agency or affiliated non-federal agency and denial is allowed under that Act.
5. Was received from a source requesting confidentiality or anonymity, and allowing access would reveal that source. This reason does not apply to a health care provider.
6. Is likely to endanger or cause substantial harm to the individual or another person, according to a decision by a licensed health care professional. (An appeal of the decision must be allowed.)

PROCEDURE

1. All requests for PHI access must be submitted in writing on the Request to Access Health Information form.
2. When the written request is received, it is routed to the Privacy Officer.
3. The Privacy Officer will review the form and determine whether the request will be accepted or declined for one of the reasons listed under Policy.
4. The Privacy Officer will respond in writing to the individual within 30 days of receipt of the request by completing the Health Plan Review/Reply section of the form and sending a copy of the entire form back to the individual.
5. If the request is approved, the Privacy Officer will request that the appropriate reports be run and/or files be copied and mailed to the individual within 30 days of approving the request.
6. The request and response will become part of the individual's file and will be maintained for a period of at least 6 years.

TEXT of PHI Access Request Form

REQUEST TO ACCESS PROTECTED HEALTH INFORMATION

Name:_____ Enrollee #:_____

As provided for by the Health Insurance Portability and Accountability Act (HIPAA), I am exercising my right to access my protected health information (PHI). I understand that information requested below will be provided to me in the form of a paper report and that I will not be charged for this service.

INFORMATION DATES

Please indicate the dates associated with the requested PHI:

Start Date:_____ through End Date:_____

TYPE OF INFORMATION REQUESTED

Please check the boxes below that apply to the type of PHI you want to access:

- ❑ Enrollment records
- ❑ Premium/contribution payment records
- ❑ Underwriting records
- ❑ Claim payment records
- ❑ Case Management/Utilization Review records
- ❑ All of the above

_____ _____

Signature of Patient or Patient's Authorized Representative **Date**

_____

If signature is Authorized Representative's, please indicate relationship or authority to act for individual.

HEALTH PLAN REVIEW/REPLY SECTION

This section is for use by authorized representatives of the group health plan only.

Date Received:_____

Title of Reviewer:_____ Date:_____

This request for access to PHI is being:

- ❑ Approved. Paper copies of the requested information will be mailed to you within 30 days. You will not be charged for this service.

- ❑ Declined, as allowed under the Health Insurance Portability and Accountability Act (HIPAA), because the information requested:

  - ❑ Is psychotherapy notes.
  - ❑ Has been compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding.
  - ❑ Is subject to the Privacy Act, 5 U.S.C. §552a, and the denial meets the requirements of that law.
  - ❑ Was received from a source, other than a health care provider, that requested confidentiality and the access would be reasonably likely to reveal that source.
  - ❑ Has been determined by a licensed health care professional as likely to endanger the life or physical safety of the individual or another person.
  - ❑ Has been determined by a licensed health care professional as likely to endanger or cause substantial harm to another person referenced in the information.
  - ❑ Was requested by a personal representative and a licensed health care professional has determined that access is likely to cause substantial harm to the individual that is the subject of the information or another person.

  If the reason for denial marked above involved a decision by a licensed health care professional regarding potential harm to yourself or another person, you have a right to have that decision reviewed. If you wish to appeal the decision, please submit a written request to have the decision reviewed. The decision will be reviewed by a licensed health care professional that was not involved in the original decision and a response will be provided to you within 30 days of receipt of your appeal.

If you believe your privacy rights have been violated, you may file a complaint with the plan or the Secretary of Health and Human Services. Complaints should be filed in writing and sent to the [**INSERT COMPANY NAME**]. The plan will not retaliate against you for filing a complaint.

REQUEST TO AMEND PROTECTED HEALTH INFORMATION

WHAT IS IT?

HIPAA guarantees individuals the right to have their protected health information (PHI), as maintained in a designated record set, amended if it is incorrect.

POLICY

Upon written request, incorrect data in our files will be amended. Records subject to amendment include:

1. Claim records.
2. Enrollment records.
3. Underwriting files, including medical records obtained.
4. Case management and utilization review/precertification files.

Requests to amend PHI will only be denied if it is determined that:

1. The group health plan did not create the information. However, if the creator of the information is shown to be unavailable to act on the request to amend, we will consider the request as if we were the creator of the information.
2. The information is not part of a designated record set listed above.
3. We are not required to make the information available to the individual for inspection. (See Policy on Requests to Access Protected Health Information.)
4. The information is accurate and complete as stated in our records.

All future disclosures of information that are associated with a request for amendment, whether accepted or denied, will include the request for amendment, the plan's decision on the request, and any rebuttal to the plan's decision. If a standard Electronic Data Interchange (EDI) transaction does not allow for the inclusion of this information, it will be provided separate from the transaction.

PROCEDURE

Requests from Individuals to Amend

1. All requests to amend PHI must be submitted in writing on the PHI Amendment Request Form.
2. When the written request is received, it is routed to the Privacy Officer.
3. The Privacy Officer will review the form and determine whether the request will be accepted or declined for the reasons listed under Policy.
4. The Privacy Officer will respond to the individual within 60 days of receipt of the request for amendment by completing the Health Plan Review/Reply section of the form and sending a copy of the entire form back to the individual.
5. If the request is being accepted, the Privacy Officer will:
    a. Identify the records affected by the amendment and request that the amendment be included or linked to those records.
    b. Provide written notice of the amendment to any person listed as requiring notification of the amendment.

c. Provide written notice of the amendment to any Business Associate or agent that the plan knows was provided the original information and who may rely on it to the detriment of the subject individual.

6. If a rebuttal to a denial is received, the Privacy Officer will document its receipt.
7. The request, response and any rebuttal will become part of the subject individual's file and will be maintained for a period of at least 6 years.

Notice from Other Covered Entities to Amend

1. All notices to amend PHI must be in writing and identify the specific information to be amended.
2. When the written request is received, it is routed it to the Privacy Officer.
3. The Privacy Officer will:
   a. Identify the records affected by the amendment and request that the amendment be included or linked to those records.
   b. Provide written notice of the amendment to any Business Associate or agent that the plan knows was provided the original information and who may rely on it to the detriment of the individual.
4. The request will become part of the individual's file and will be maintained for a period of at least 6 years.

TEXT of PHI Amendment Request Form

REQUEST TO AMEND PROTECTED HEALTH INFORMATION

Name:_____ Enrollee #:_____

As provided for under the Health Insurance Portability and Accountability Act (HIPAA), I am exercising my right to request that my protected health information (PHI) be amended as indicated below.

AMENDMENT REQUEST

Information to be Amended

Describe/identify the information that you are requesting be amended:_____

_____

Indicate the reason(s) why you believe the information is incorrect in our files:_____

_____

_____

Indicate what you believe the correct information to be:_____

_____

_____

Indicate the name and address of anyone you are requesting be notified of this correction:

_____

_____

_____

_____

_____ _____

Signature of Patient or Patient's Authorized Representative **Date**

_____

If signature is Authorized Representative's, please indicate relationship or authority to act for individual.

HEALTH PLAN REVIEW/REPLY SECTION

This section is for use by authorized representatives of the group health plan only.

Date Received:_____

Title of Reviewer:_____ Date:_____

This request for amendment of PHI is being:

- ❑ Approved.
- ❑ Declined because the plan did not create the information. However, if the creator of the information is unavailable to act on the request to amend, please notify the plan in writing and we will reconsider the request.
- ❑ Declined because the information is not part of a designated record set the plan maintains.
- ❑ Declined because we are not required to make the information available to the individual for inspection.
- ❑ Declined because the information is accurate and complete as stated in the plan's records.

All future disclosures of this information will include your request to amend it and our decision as indicated above.

If you disagree with this decision, you have the right to file a limited (one page or less) rebuttal to the decision that will be included with any future disclosures of the information.

If you believe your privacy rights have been violated, you may file a complaint with the plan or the Secretary of Health and Human Services. Complaints should be filed in writing and sent to [**INSERT COMPANY NAME**]. The plan will not retaliate against you for filing a complaint.

REQUEST FOR ACCOUNTING OF DISCLOSURES

WHAT IS IT?

HIPAA guarantees every individual the right to a listing or accounting of the disclosures of their protected health information (PHI) for a period of up to 6 years prior to the request, with the exception of disclosures made:

1. To carry out the functions of treatment, payment and health care operations.
2. Under a signed HIPAA Authorization.
3. To the individual that is the subject of the information.
4. That are incidental to a use or disclosure otherwise permitted under the regulation.
5. As part of a limited data set.
6. To persons involved in the individual's care or for notification purposes.
7. For national security or intelligence purposes.
8. To correctional institutions or law enforcement officials.
9. Prior to the covered entity's compliance date for the HIPAA regulation (4/14/2004).

As defined in HIPAA, payment and health care operations include the following activities:

1. Activities to obtain premiums or to determine or fulfill the plan's responsibility for coverage and payment of benefits;
2. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost-sharing amounts), and adjudication or subrogation of health benefit claims;
3. Risk-adjusting amounts based on enrollee health status and demographic characteristics;
4. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
5. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
6. Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services;
7. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: name and address; date of birth; social Security Number; payment history; account number; and name and address of the health care provider and/or health plan;
8. Quality assessment, protocol development, case management, and provision of information about treatment alternatives;
9. Evaluation of provider or health plan performance;
10. Underwriting, premium rating, and other activities relating to the placement of a contract of health insurance or health benefits, including obtaining reinsurance, stop-loss/excess-loss insurance for the plan;
11. Conducting or arranging for medical review, legal services, and auditing functions;
12. Business planning and development, such as conducting cost-management and planning-related analyses; and
13. Business management and general administrative activities of the entity.

POLICY

An accounting of disclosures of PHI will not be made if the disclosures fall within the exceptions listed above.

PROCEDURE

1. All requests for accounting must be in writing.
2. When the written request is received, it is routed to the Privacy Officer.
3. The Privacy Officer will respond in writing to the individual within 30 days of receipt of the request by sending the PHI Accounting Request Letter.
4. The request and response will become part of the individual's file and will be maintained for a period of at least 6 years.

TEXT of PHI Accounting Request Letter

RE: Request for Accounting of Protected Health Information

Dear _____,

We have received your request to account for disclosures of protected health information (PHI).

The Health Insurance Portability and Accountability Act (HIPAA) does not require an accounting of disclosures made:

1. To carry out the functions of treatment, payment and health care operations.
2. Under a signed HIPAA Authorization.
3. To the individual that is the subject of the information.
4. That are incidental to a use or disclosure otherwise permitted under the regulation.
5. As part of a limited data set.
6. To persons involved in the individual's care or for notification purposes.
7. For national security or intelligence purposes.
8. To correctional institutions or law enforcement officials.
9. Prior to the covered entity's compliance date with the HIPAA regulation (4/14/2004).

As stated in our Privacy Notice, the plan does not provide an accounting of disclosures of PHI that fall within the exceptions listed above.

Sincerely,

PRIVACY COMPLAINT PROCESS

POLICY

The Office to Receive Privacy Complaints is responsible for receiving and responding to all privacy complaints. All complaints, verbal or written, will be referred to this office. The office will document and respond to all complaints.

PROCEDURE

1. Privacy complaints should be routed to the Office to Receive Privacy Complaints.
2. The complaint will be researched to determine its validity.
3. If the complaint is valid, it will be reported to the Privacy Officer and Human Resources Department (HR).
4. The Privacy Officer in connection with HR will determine if employee sanctions are appropriate and enforce them according to company policies.
5. The Privacy Officer will determine if mitigation of any harm is appropriate and possible.
6. The Privacy Officer will respond to the complaint in writing within 30 days.
7. The Privacy Officer will maintain the complaint, any information collected in researching it and the final response to it for a period of at least 6 years.

PRIVACY NOTICE QUESTIONS AND INFORMATION

POLICY

The Privacy Officer is responsible for responding to all inquiries regarding the company's Privacy Notice.

PROCEDURE

1. The Privacy Officer will respond to any inquiry regarding the company Privacy Notice by providing the requested information or explanation within 30 days of our receipt of the inquiry.

EMPLOYEE SANCTIONS

POLICY

All accusations of employee violations of company Privacy Policy will be reviewed by HR and the Privacy Officer. If it is determined that a violation has occurred, HR and the Privacy Officer will jointly decide if it was an intentional or unintentional violation and apply sanctions as outlined below.

PROCEDURE

Intentional Violations of Privacy Policy

Violations of the company's stated Privacy Policy that are determined to be intentional will result in the immediate termination of the employee's employment.

Upon determining that an intentional violation has occurred:

1. HR will terminate the employee's employment.
2. The Privacy Officer will determine the need to mitigate any damages as possible and take appropriate action.

Unintentional Violations of Privacy Policy

Violations of the company's stated Privacy Policy that are determined to be unintentional will be handled through the standard disciplinary process:

1. Verbal warning — first Privacy Policy violation.
2. Written warning — second Privacy Policy violation.
3. Termination of employment — third Privacy Policy violation.

Depending on the nature and severity of the violation, the company has the discretion to alter the disciplinary steps listed above.

Note: Repetition of an unintentional violation of Privacy Policy after it has been addressed with the employee will be considered an intentional violation and subject the employee to termination of employment.

1. HR will take appropriate disciplinary action as outlined above.
2. The Privacy Officer will determine the need to mitigate any damages and take appropriate action.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

POLICY

Appropriate administrative, technical and physical safeguards will be maintained to ensure the protection of information received, maintained and disclosed, as required by HIPAA. Safeguards will account for the nature of the information, where it is located (secured building with only employee access, at-home worker, in transit from one location to another, etc.), and its various formats and media.

PROCEDURE

Physical Safeguards

1. All paper file systems will be secured in a locked area or locked file cabinets during non-working hours. Access will be limited based on job class and need.
2. Fax machines will be secured in a locked area during non-working hours. Access will be limited based on job class and need.
3. Employees with access to PHI will secure any PHI at their workstation in a locked file cabinet or overhead bin prior to leaving for the day. At-home workers and employees who bring work home will secure any PHI at their home when it is not being used for business purposes.
4. All electronic transmissions (fax or email) of PHI will include a company-approved statement of confidentiality.
5. All printed material containing PHI will be placed in envelopes in such a way that no PHI is visible.
6. All paper documents containing PHI will be shredded prior to disposal for recycling.
7. Material containing PHI will not be left unattended in common areas such as copy rooms.

Technical Safeguards for Employees With Access to PHI

1. All PCs and laptops will be equipped with auto log-off features to close programs with access to PHI after a set period of inactivity.
2. All laptops will have encryption and password protocols to prevent unauthorized access to data on the drives of the laptop.

Administrative Safeguards

1. All employees, including management personnel, will receive training on the HIPAA Privacy and Security Rules and company policies on privacy and security.
2. Upon termination of any system user, access for that user will be removed immediately.
3. Transport and disposal of all media types (diskettes, tapes, email, laptops, etc.) will conform to approved Media Control Policies to ensure that PHI is removed.
4. Access to PHI in electronic systems and file storage will be limited through job based access standards, as documented under Procedure in Minimum Necessary Rule.
5. Employees will not disclose PHI in any format or manner (electronic, paper or verbal) except as necessary for business reasons and in compliance with the Minimum Necessary Policy of the company. This includes external disclosures and internal disclosures to other employees.

DOCUMENTATION

WHAT IS IT?

HIPAA requires that documentation of all personnel designations and actions required by the Privacy Rules be documented and maintained for a period of six years from the later of the date it was created or the date it was last modified.

POLICY

Documentation required by the HIPAA Privacy Rules will be maintained [**INSERT A DESCRIPTION OF YOUR COMPANY'S FILE DOCUMENTING SYSTEM**].

All records will be maintained for a period of six years from the date they were created or modified.