MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN
PRIVACY POLICIES AND PROCEDURES

I. GENERAL PRINCIPLES

The health plan is committed to protecting the privacy of member's protected health information in accordance with federal and state regulations consistent with the delivery of a quality health plan, effective management of health care operations, and payment of covered health care services. These Montgomery County Employee Benefit Plan (health plan) policies and procedures implement privacy protections in accordance with the Health Insurance Portability and Accountability Act of 1996, Privacy Regulations, (Privacy Regulations) promulgated by the Secretary of the U. S. Department of Health and Human Services at 45 C.F.R. Subtitle A, Subchapter C.

II. PURPOSE AND SCOPE

The purpose and scope of these policies and procedures is to delineate the privacy policies of the health plan and the procedures for implementing the policies to achieve compliance with the Privacy Regulations.

III. PROTECTED HEALTH INFORMATION DEFINITION:

Protected health information ("PHI") is any individually identifiable health information that is transmitted or maintained in any form, including demographic information collected from an individual, and:

Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

IV. DESIGNATION OF PRIVACY OFFICER

The Privacy Officer for the health plan is:

Director of Risk Management, Privacy Officer
501 North Thompson, Suite 202
Conroe, Texas 77301,
(936) 760-6935

The Privacy Officer has overall responsibility for administering the policies and procedures to assure compliance with the Privacy Regulations. Additionally, the Privacy Officer is the designated authority to receive and process: (i) complaints, (ii) requests for copies of PHI, (iii) requests for communications by alternative means or alternative locations (confidential communications), (iv) subpoenas and other requests from judicial authorities, and (v) other correspondence and matters related to the privacy of PHI.

Complaint Filing Procedures

The Privacy Officer is designated to receive complaints filed with the health plan regarding the health plan's policies and procedures and its compliance with those policies and procedures. Complaints must be filed in writing and directed to the Privacy Officer. The writing must contain a description of the complaint and an explanation of the circumstances surrounding the complaint. The health plan is not required to respond to complaints, but the Privacy Officer shall be responsible for documenting receipt of a complaint and any resolution. A complaint form is attached hereto as Attachment A.

Complaints may also be filed with the Secretary of the U.S. Department of Health and Human Services (referred to herein as the Secretary). No retribution or negative action will be taken or tolerated because a member files a complaint with the health plan or the Secretary.

V. NOTICE OF PRIVACY PRACTICES - SYNOPSIS

Each employee will receive a Notice of Privacy Practices ("the Notice") from the health plan. However, we have provided below a summary of some of the important points contained in the Notice.

The health plan generally uses and discloses PHI only in furtherance of providing the medical and/or dental benefits described in the health plan's specific benefit document. The health plan uses and discloses the PHI to process requests for payment, to respond to eligibility and benefit inquiries from providers, and for other reasons related to the operation of the specific benefit plan, (these reasons are described in the Notice as "health care

operations"). The health plan contracts with business associates to performvarious services or to perform certain specified functions, such as administration of claims, member service support, utilization management, subrogation, pharmacy benefit management, stop-loss insurance and other similar functions. The health plan utilizes these business associates to receive, create, maintain, use, and disclose relevant PHI for the purposes of treatment, payment of health claims and health care operations.

The health plan requires each business associate to adopt the health plan's Privacy Policies and Procedures or a similar set of policies and procedures that meet the same objectives required by the Privacy Regulations.

The health plan discloses PHI to the plan sponsor for the purpose of plan administration functions, including funding benefits and determining the health and viability of the health plan. The plan sponsor has certified that, among other actions, it has limited the access to PHI to relevant personnel and that PHI will not be used in any employment action or in connection with any other plan sponsor benefit.

Periodically the health plan requests proposals from insurance and stop-loss companies to ensure the viability of the health plan. In the course of developing proposals, occasionally specific PHI is required by stop-loss companies and others. The health plan assists in providing the required information in furtherance of its responsibility to maintain plan integrity and fiscal health. Stop-loss companies are included in the health plan's business associates and, as such, will comply with the rules set forth in these policies and procedures for business associates.

The health plan may disclose PHI to various health care providers for the purpose of treatment, payment, for services to plan members, or in furtherance of disease management or other health care operations of the health plan.

VI. RETENTION OF DOCUMENTATION

Documentation required by the Privacy Regulations, shall be maintained for six (6) years from the date a document is created or the date when it was last in effect, whichever is later.

A database for retaining required documentation has been created. Required documentation shall be entered in the electronic database and retained for six (6) years from the date a document is created or the date when it was last in effect, whichever is later, beginning with the required compliance date of the Privacy Regulations. The Privacy Officer shall be responsible for assuring that relevant data is entered promptly.

Where electronic copies are not available or actual practice requires paper copies of documents, the paper copies shall be securely maintained for the required six (6) years. The Privacy Officer shall maintain a list of documents that must be retained in paper form. Once the Secretary adopts an electronic signature regulation and compliance with that regulation is required, future paper documents may be converted and retained electronically in the tracking database.

VII. MEMBER PRIVACY RIGHTS

Policy

Members generally have the following rights.

The right to request restrictions on certain uses and disclosures of PHI. However, the health plan is not obligated to agree to a requested restriction.

The right to receive confidential communications of PHI, provided that the member: (i) describes in writing the desired alternative location for, or alternative means of, communication, and (ii) indicates in the writing that the disclosure of the PHI in a manner inconsistent with the request could endanger the individual.

The right to inspect and copy most PHI contained in a designated record set.

The right to request amendment of PHI; however, the health plan is not obligated to agree to a requested amendment.

The right to receive an accounting of disclosures of PHI for most purposes other than for treatment, payment, or health care operations.

The right to obtain a paper copy of the Notice of Privacy Practices even if previously agreeing to receive such notice electronically.

Procedures

Member Requested Restrictions

The health plan shall monitor and maintain a log of requests for restrictions on uses and disclosures of PHI. The Privacy Officer shall be responsible for determining the reasonableness of all requests, and for conveying in writing the health plan's decision on such requests.

A log shall be maintained of such requests and the disposition of such requests.

The member shall be notified of the decision concerning the requested restriction.

The Privacy Officer is not obligated to agree to such requests but shall include in the consideration of a request the impact and feasibility of such request in view of difficulties or disruptions that may result on plan administration.

If the Privacy Officer agrees to a request for restriction, the Privacy Officer will:

Document such restriction and maintain it in accordance with the Retention of Documentation policy and procedures; and

Take the appropriate and necessary steps to ensure that the health plan complies with the restriction.

Even if the health plan has agreed to a restriction, the health plan may disclose the restricted PHI to a health care provider for emergency treatment of the individual.

The Privacy Officer may terminate a restriction, if:

The member requests or agrees (in writing or orally) to terminate the restriction (an oral agreement to terminate restriction must be documented); or

The Privacy Officer informs the member that the restriction is terminated with respect to PHI received or created after the effective date of the termination.

Confidential Communications with Members

A member may request in writing confidential communications if the disclosure of PHI could endanger the member.

The written request shall be sent to the Privacy Officer and must: (i) specify in writing the alternative address or alternative means for confidential communications, and (ii) state that the disclosure of the PHI in a manner inconsistent with the request could endanger the member.

The Privacy Officer will accommodate a reasonable request by a member to receive communications regarding his/her PHI in an alternative manner or at an alternative location when disclosure of the PHI in a manner inconsistent with the member's request could endanger the member.

The Privacy Officer will take the appropriate and necessary steps to ensure that the health plan complies with any approved request for confidential communications.

Right of Access

Members have the right to request in writing a copy of their PHI maintained by the health plan in designated record sets. 'Designated record set' is a term of art that is defined in the Privacy Regulations. The designated record sets shall generally only include claims history, payments, benefits, and eligibility. A member has a right to access, inspect, and obtain a copy of PHI about the member maintained in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

Psychotherapy notes;

Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or

PHI maintained by a Covered Entity that is:

Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the member would be prohibited by law; or

Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a) (2).

Members may request information by submitting a written request to the Privacy Officer.

If the requested information is on site at the health plan, the request will be honored or denied within thirty (30) days of receipt.

If some or all of the requested information is not on site, or is maintained by a business associate, the request will be honored or denied within sixty (60) days. An approved request shall be forwarded promptly to the relevant business associates.

If necessary, the Privacy Officer may take one extension of thirty (30) days in which to make access available. The Privacy Officer shall send a written notice to the member of the delay with the reasons for the delay and the date by which the member will be allowed access. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures.

If the request is granted in whole or in part, the Privacy Officer will inform the member that the request has been granted in whole or in part.

The Privacy Officer will establish the amount of the charge for copying the requested information, if there is to be a charge. If established, the charge shall be based only on actual costs. The costs to be considered shall be the cost of supplies, labor for copying, preparation of the information, and postage if mailed. The Privacy Officer will communicate to the member the charge for copying the requested information. The Privacy Officer may from time to time establish the appropriate charge for copying the requested information. Such established charges shall be reviewed at least annually to verify they are reflective of actual costs.

If the request is denied in whole or in part the Privacy Officer shall provide written notice of the denial in plain language and include: (i) the reasons for the denial, (ii) an explanation of the member's right for a review of the denial, and (iii) a description of how the member may file a complaint with the health plan or the Secretary of the U. S. Department of Health and Human Services ("DHHS"). The denial shall be maintained in accordance with the Retention of Documentation policy and procedures.

If the reason for denial is that the information is not maintained by the health plan, the Privacy Officer shall direct the member to where the information may be obtained, if such location is known by the health plan.

If the member requests in writing a review of the denial, the request will be forwarded for review and resolution to a designated licensed health care professional who has not been directly involved with the review process resulting in the denial.

The designated reviewing health care professional shall, within a reasonable time, review the denial in accordance with the standards established in Section 164.524(a) (3) of the Privacy Regulations.

The results of the review will be sent to the member in a written notice and the health plan will take appropriate action to follow the health care professional's determination. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures.

Right to Request Amendment

Members have the right to request an amendment to their PHI maintained by the health plan.

Members may request amendment of information by submitting to the Privacy Officer the Amendment Request Form attached hereto.

The health plan will act upon the request within sixty (60) days of receipt.

If necessary, the Privacy Officer may take one extension of thirty (30) days in which to determine whether to make an amendment. The Privacy Officer will send a written notice to the member of the delay with an explanation of why the delay is required, and the date by which a decision will be made regarding the requested amendment. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures.

If the request for amendment is accepted, the health plan shall:

Identify the designated record set(s) in which the PHI that is the subject of the amendment request is contained and make the amendment;

Inform the member that the amendment is accepted;

Obtain from the member the names and addresses of persons to whom the amended information should be sent;

Once agreement is obtained from the Member:

Make reasonable efforts to provide the persons identified by the member with the amended information; and

Make reasonable efforts to provide the amended information to other relevant persons and business associates: (i) that have the PHI that is the subject of the amendment; and (ii) that may have relied or could rely on the PHI to make a decision about the member.

If the request is denied in whole or in part, the Privacy Officer shall provide a written notice of the denial and include:

The reasons for denial;

The member's right to submit a statement disagreeing with the denial;

How the member may submit the statement of disagreement;

A statement that the member may request the health plan to include the member's request for amendment and its denial with any future disclosures of the disputed PHI, in lieu of submitting a statement of disagreement; and

A clear statement of the member's right to complain to the health plan and to the Secretary of DHSS.

The denial shall be maintained in accordance with the Retention of Documentation policy and procedures.

The health plan, at its option, may prepare a rebuttal statement.

Upon the request of the member, any future disclosures will include the request for amendment and the denial.

Any future disclosures will include any statement of disagreement and rebuttal.

The Privacy Officer will maintain a log of all requests for amendment and the applicable resolutions.

When another covered entity sends the health plan amended PHI, the Privacy Officer will ensure that the health plan takes all appropriate and necessary steps to amend the PHI that it maintains in designated record set(s).

VIII. DISCLOSURES AND USES OF PROTECTED HEALTH INFORMATION

The health plan will not obtain a consent or authorization to use and disclose PHI to carry out treatment or payment or health care operations.

When the use and disclosure of PHI is not for treatment, payment, health care operations, or otherwise permitted or required by law without an authorization, the health plan will obtain a valid authorization from themember prior to using or disclosing PHI. Specifically, an authorization may be obtained for FLEX administration, Long Term Disability, Medical and Family Leave Act requests and other similar operations when offered or the request requires release of health plan PHI.

There will not be a health plan authorization for information containing PHI when it comes directly from the employee and not the health plan. For example, a doctor's note describing a condition supporting a disability claim that did not originate from the health plan will not require a health plan authorization.

There will not be a health plan release for employer mandated health activities, such as work place drug testing, workers' compensation, ADA or OSHA.

When the health plan receives an authorization for disclosures from another entity or person, the Privacy Officer will review the authorization to determine: (i) that it is a valid authorization pursuant to Section 164.508 of the Privacy Regulations, and (ii) the minimum amount of information that is necessary to disclose to comply with the authorization.

IX. CLASSES OF USERS OF PROTECTED HEALTH INFORMATION

All of the classes of PHI within the health plan are also employees of the plan sponsor. Classes of users of PHI are to have access to the minimum amount of PHI reasonably necessary to perform their functions and responsibilities. The classes of persons within the health plan who need access to PHI to carry out their duties, along with the conditions of access and the uses of such information, are as follows:

CLASSES

Risk Management Analyst

Risk Management analysts shall have access to PHI as needed for processing health claims, eligibility, benefits, and facilitating healthcare operations. Analysts include those that administer, approve payment, process, or facilitate processing of health claims, eligibility, benefits including medical, dental or other claims or benefits. This class also includes those responsible for interacting with members, employees, providers, business associates and others in resolving eligibility, benefit, claims, coordination of benefits and other plan administration issues.

Information Technology

IT personnel include system technicians responsible for organization web sites, connectivity within the organization's networks, email and for connectivity with external networks.

Financial Accountants

Financial Accountants shall have access to PHI as necessary to reconcile banking and other financial statements and to process financial functions necessary to the health plan.

Attorneys

Attorneys and the administrative staff of the County Attorneys office shall have access to defend claims against the Montgomery County Employee Benefit plan.

X. PROTECTION OF PROTECTED HEALTH INFORMATION

Access by the various classes of PHI users shall be limited to the minimum necessary amount of PHI information reasonably calculated to allow performance of their duties.

Access by the various classes of PHI users shall be limited and controlled by network passwords. Access to PHI will be limited to those classes of users requiring the information.

Appropriate physical safeguards shall be observed. Physical copies of records and reports containing PHI shall be maintained in secure filing cabinets, locked drawers or locked rooms and not left open or available for inadvertent exposure.

Documents containing PHI shall not be left out on desks or in other areas where there is a significant danger of inadvertent disclosure.

At the end of the workday documents containing PHI shall be filed in locked filing cabinets, locked desks or locked offices.

Staff involved in opening and sorting mail shall identify mail that contains PHI and shall route it to appropriate personnel. Mail or other documents containing PHI shall be processed timely and not left out where there is significant danger of inadvertent disclosure.

XI. ROUTINE DISCLOSURES AND REQUESTS OF PROTECTED HEALTH INFORMATION

The health plan generally discloses PHI only in furtherance of providing the medical and/or dental benefits described in the health plan's specific benefit document. The health plan discloses the PHI to process requests for payment, to respond to eligibility and benefit inquiries from providers, and for other reasons related to the operation of the specific benefit plan (these reasons are described in the Notice as "health care operations"). The health plan contracts with business associates to perform various services or to perform certain specified functions, such as administration of claims, member service support, utilization management, subrogation, pharmacy benefit management, and other similar functions. The health plan utilizes these business associates to receive, create, maintain, use, and disclose relevant PHI for the purposes of treatment, payment of health claims and health care operations.

Periodically the health plan requests proposals from insurance and stop-loss companies to ensure the viability of the health plan. In the course of developing proposals, occasionally specific PHI is required by stop-loss companies. The health plan assists in providing the required information in furtherance of its responsibility to maintain plan integrity and fiscal health. Stop-loss companies are the health plan's business associates and, as such, will comply with the rules set forth in these policies and procedures for business associates.

The health plan may disclose PHI to various health care providers for the purpose of treatment, payment, services to plan members, or in furtherance of disease management or other health care operations of the health plan.

The health plan discloses information to the plan sponsor for the purpose of funding benefits and determining the health and viability of the health plan. The plan sponsor has certified that, among other actions, it has limited the access to PHI to relevant personnel and that PHI will not be used in any employment action or in connection with any other plan sponsor benefit.

In general, the health plan will request PHI on a routine basis only for those purposes described in paragraphs A through D above. Where the health plan requests PHI from a member, a non-covered entity, or another covered entity, it will limit its request to the amount of PHI necessary to accomplish those purposes outlined above (*i.e.*, in paragraphs A through D).

The health plan will not disclose or request an entire medical record unless the entire record is reasonably necessary to accomplish the purpose of the disclosure or request.

XII. NON-ROUTINE DISCLOSURES AND REQUESTS OF PROTECTED HEALTH INFORMATION

The Privacy Officer will review each non-routine disclosure on an individual basis. The Privacy Officer will determine the minimum amount of PHI necessary for the disclosure, using established criteria that includes, but is not limited to:

Identifying the type of PHI requested (*e.g.*, demographic, diagnosis, or procedures information); and

Evaluating the purpose for the disclosure (*e.g.*, treatment, payment, or health care operations).

The health plan may rely on public officials and other covered entities under the Privacy Regulations to request only the minimum necessary amount of PHI.

Where the health plan is requesting PHI on a non-routine basis, the Privacy Officer will review the request to ensure that the health plan is limiting its request to only the information it reasonably needs to accomplish the purpose of the disclosure or request.

The health plan will not disclose or request an entire medical record unless the entire record is reasonably necessary to accomplish its purpose.

XIII. VERIFYING IDENTITY AND AUTHORITY PRIOR TO DISCLOSURES

Where the health plan does not know the identity of the individual or entity (including public officials), it shall use its professional judgment to verify the identity and the authority of the individual or entity before disclosing the requested PHI unless the disclosure is for one of the reasons identified in § 164.510 of the Privacy Rule (*e.g.*, in an emergency).

If the Privacy Regulations require documentation, statements, or representations (*e.g.*, subpoena, authorization, and government letterhead) as a condition of making a disclosure, the health plan may rely on such materials to make the disclosure of PHI without performing additional verification, unless otherwise required by the Privacy Regulations or other law.

With respect to disclosures to public officials, the health plan may rely on the following to verify:

Public official's identity:

If the request for PHI is made in person, agency identification, badge, or other proof of government status;

If the request for PHI is made in writing, the request is on government letterhead; or

If the request is to an entity or individual acting on behalf of a government entity, documentation that the entity or individual is acting on behalf of the government entity.

Public official's authority:

A written or oral statement of legal authority for the disclosure of PHI; or

A warrant, subpoena, administrative or court order, or other legal process that provides legal authority for the disclosure.

XIV. DISCLOSURES TO BUSINESS ASSOCIATES

The health plan uses business associates that are not part of the health plan workforce to carry out various health plan functions of payment for medical services and health care operations. These functions may include but are not limited to administration of claims, member service support, provider relations, utilization review, pharmacy benefit managers, subrogation, stop-loss companies, and other necessary activities.

Business Associate Procedures

Each Business Associate will adopt privacy policies and procedures acceptable to the health plan. The policies and procedures will be referenced in the business associate agreement and will be either identical to these policies and procedures or approved by the Privacy Officer as complying with the HIPAA Privacy Regulations.

It is reasonable to presume the PHI requested by a business associate be the minimum information necessary required to perform the business associate task(s). The Privacy Officer may rely on requests of business associates as being requests for the minimum necessary amount of PHI.

Each business associate agreement or subcontract shall contain an obligation to use the PHI only for the purposes and functions required by the health plan, and only as long as there is relation to the health plan.

The Privacy Officer shall review at least annually the business associate's policies and procedures regarding recurring information disclosures for appropriateness and to ascertain that the minimum necessary is being disclosed.

The Privacy Officer will consider the following factors in reviewing and approving the business associate's policies and procedures regarding recurring disclosures of PHI:

The nature of the PHI: such as whether it is benefit information, claims history, eligibility, diagnoses, procedures, or other relevant categorizations;

The functions performed by the business associate; and

Whether the entity or business associate is engaged in a pattern of activity that constitutes a material breach or violation of the Business Associate agreement.

XV. DISCLOSURES TO PLAN SPONSOR AND PLAN SPONSOR AGENTS

The health plan will not disclose PHI to the plan sponsor except upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions or other provisions that achieve the same HIPAA compliance objectives, and that the plan sponsor agrees to:

Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

Ensure that any agents, including a subcontractor, to whom it provides PHI received from the health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor; and

Report to the health plan any inappropriate use or disclosure of which it becomes aware that is inconsistent with the uses or disclosures provided for.

The plan document must:

Describe permitted uses of PHI;

Specify that the plan sponsor has provided required certification, which includes the ten points identified below;

Ensure firewalls have been established. A firewall, in this regard, means procedural and policy limitations on which plan sponsor personnel can receive PHI and the specific limits on use of the PHI. A firewall is a clear delineation of the permissible uses of, and individual authority to use, PHI;

The health plan will rely on a certification from the plan sponsor that the plan sponsor will handle disclosures of PHI to the plan sponsor as follows:

Not further use or disclose PHI other than as permitted or required by plan document or as required by law,

Ensure subcontractors agree to the same,

Not use PHI for employment-related actions,

Report any inconsistent use or disclosure,

Allow individuals to request amendments of their PHI,

Provide an accounting of disclosures unrelated to payment or health care operations

Make practices available to the Secretary for compliance,

If feasible, return or destroy all PHI when use is finished, and

Ensure firewalls are established. Firewalls will establish the classes of individuals at the plan sponsor that have access to PHI and the criteria to determine use of PHI.

C. Security Standards

1. Plan Sponsor Obligations -

Where Electronic Protected health Information will be created, received, maintained, or transmitted to or by the plan sponsor on behalf of the Plan, the Plan sponsor shall reasonably safeguard the Electronic Protected Health Information as follows:

a. Plan sponsor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that Plan sponsor creates received, maintains, or transmits on behalf of the Plan;

b. Plan sponsor shall ensure that the adequate separation that is required by 45 C.F.R. § 164.504(f)(2)(iii) of the HIPAA Privacy Rule is supported by reasonable and appropriate security measures;

c. Plan sponsor shall ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate security measures to protect such Information; and

d. Plan sponsor shall report to the Plan any Security Incidents of which it becomes aware as descried below:

i. Plan sponsor shall report to the plan within a reasonable time after Plan sponsor becomes aware, any Security Incident that results in unauthorized access, use, disclosure, modification, or destruction of the Plan's Electronic Protected Health Information; and

ii. Plan sponsor shall report to the Plan any other Security Incident on an aggregate basis every month, or more frequently upon the Plan's request.

XVI. JUDICIAL, ADMINISTRATIVE AND GOVERNMENTAL DISCLOSURES

Disclosures of PHI may be made in the following instances:

In response to a court order or administrative tribunal provided that only the PHI expressly authorized by the order would be disclosed.

In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

a. The health plan receives satisfactory assurance from the party seeking the information that reasonable efforts were made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request. Satisfactory assurance means:

The requesting party has mailed a written notice to the individual's last known address;

The requesting party provides the health plan a written statement, with accompanying documentation, demonstrating that the notice was given and that it contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection with the court or tribunal; and no objections were raised or all objections were resolved.

The health plan receives satisfactory assurance that the party requesting the PHI has made reasonable efforts to obtain a protective order. A qualified protective order means that the parties involved in the dispute are:

Prohibited from using or disclosing the PHI for any purpose other than the proceeding for which the information was requested; and

Required to return to the health plan or to destroy the PHI at the end of the proceeding.

In response to authorized public health requests;

For purposes of health oversight activities; and

For purposes of DHSS enforcement of Privacy Regulations.

XVII. DISCLOSURES TO MEMBERS IN FURTHERANCE OF TREATMENT, CLAIM ADJUDICATION, PRECERTIFICATION, AND OTHER PAYMENT ISSUES

Generally, health plan personnel may use, disclose, and discuss an individual's PHI with the individual. There are exceptions for psychotherapy notes and certain institutional requests.

Procedure for identifying members: A member may be identified in person by personal knowledge, government issued identification or other similar documentation. A person may be identified over the telephone. Before discussing PHI by telephone with a member or personal representative, the identity of the individual must be ascertained:

Identify the member. A member may be identified over the phone if they have the following minimum required personal information:

Member's Social Security Number,

Member's address,

Member's phone number,

In the course of a member service call or other contact with a member, the member should have knowledge available to the member of information such as:

Provider's name,

Past services,

Prior contacts, etc.

If identity of a member is not certain or becomes suspect, no PHI should be disclosed.

If the caller is inquiring about another individual, verify the right of the caller to access the requested PHI.

Generally, parents have a right to access the PHI of minor children. If there are notes in the record addressing the issue of parental rights such as limiting a non-custodial parent's right of access, the notes should be followed when determining what access a parent should have to a minor child's PHI.

As permitted by state law, if a dependent child has established with the health plan an approved mode of alternate confidential communications, disclosure of PHI to the parent may not be permitted.

It is the obligation of the requesting individual to prove their right to the PHI. This may not be possible over the phone.

XVIII. DISCLOSURES TO PROVIDERS IN FURTHERANCE OF CLAIM ADJUDICATION, PRECERTIFICATION, AND OTHER PAYMENT ISSUES

A. PHI may be discussed or disclosed to a member's health care providers in furtherance of treatment, health care operations, and payment.

B. Procedure for identifying provider in provider phone conversations.

1. Verify the identity of the individual as a provider authorized to request information or discuss the PHI. If Montgomery County personnel originate the phone conversation it may be assumed the call recipient is appropriate. For example when calling the listed number of a hospital business office it may be initially presumed the answering person is an authorized representative of the provider. A provider may be identified over the phone if the provider is known from prior contacts or has the correct

a. Provider tax ID, or

b. The member's social security number, or

c. Demonstrates knowledge of the relevant member and history.

2. If the identity or authority of the provider personnel is in doubt information should not be disclosed.

XIX. PROCEDURE FOR SENDING PHI VIA FAX:

A. The health plan has designated a certain FAX machine for sending and/or receiving PHI at each location.

B. An individual at each location has been trained and tasked to identify PHI related faxes and distribute them appropriately.

C. The FAX machine used for PHI at each location may not be secure and PHI may have to be sent with an advance call to make sure the recipient is waiting for the FAX to minimize inadvertent disclosures.

D. A Confidential Fax Coversheet to provide extra protection for PHI has been developed. The headline of the coversheet states in large bold type: "Confidential Health Information Enclosed". Beneath this headline, is a statement: "Health Care Information is personal and sensitive information related to a person's health care. It is being faxed to you after appropriate authorization from the patient/member or under circumstances that do not require patient/member authorization. You, the recipient, are obligated to maintain the health care information in a safe, secure, and confidential

manner. Re-disclosure of the health care information transmitted without additional patient/member consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law."

E. Included at the bottom of the fax coversheet is a warning: "IMPORTANT WARNING: This message is intended for the use of the person or entity to whom it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this information is STRICTLY PROHIBITED. If you have received this message by error, please notify us immediately and destroy the related message."

F. In addition to the warnings described in (4) and (5) above, the fax coversheet contains standard information including:

1. Date and time of the fax,

2. Sender's name, address, telephone number and fax number,

3. The authorized recipient's name, telephone number and fax number,

4. Number of pages transmitted, and

5. Information regarding verification of receipt of the fax.

G. Staff shall make certain the fax transmittal has received the proper authorization as required by law (i.e., that an appropriate release or authorization is on file) or that there is implied consent because the transmittal is in furtherance of treatment, health care operations or payment.

H. Faxing of sensitive health information, such as that dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information, is prohibited without supervisor approval.

I. When expecting the arrival of a fax containing PHI, coordinate with the sender whenever possible so the faxed document can be promptly retrieved upon arrival.

J. As with other PHI that arrives in the mail or by other means, make sure faxes that contain PHI are placed in the designated secure/confidential location when they are delivered, and not left in an in-box in view of passers-by.

K. Confirm the accuracy of fax numbers. It should be presumed the fax numbers provided by business associates are correct and secure. The numbers provided by recipients generally may be relied upon as valid. If there is reason to believe a number is not valid or security is suspect, the number, or security of recipient machines, should be checked by calling the intended recipients to double-check the numbers.

L. In instances where faxes are regularly sent to the same recipients, program these fax numbers into the machine's memory, using the speed-dial numbers. Programmed numbers should be tested at regular intervals.

M. Make sure fax machine prints a confirmation of each outgoing transmission and require machine operators to: (a) make sure the intended destination matches the number on the confirmation, and (b) staple the confirmation to the document that was faxed.

N. In the event of a misdirected fax, be sure that improperly faxed documents are either immediately returned or destroyed by the recipient. Document that the fax was misrouted and take (and document) steps to prevent a reoccurrence of the error.

O. Proof of delivery of PHI that is faxed, will be retained as evidence of the time/date of the transmittal, the intended recipient, its contents, and the fax number at which it was confirmed to have been received.

P. Included in the business associate agreements or two-way covered entity agreements are provisions requiring organizations that will receive your faxes to place their fax machines in secure areas.

Q. As with all other paper documents that contain PHI, faxes that contain PHI are handled and stored in the regular secure manner and shredded when they have outlived their usefulness.

XX. PROCEDURE FOR SENDING AND RECEIVING EMAIL CONTAINING PHI.

A. Email internal to the Montgomery County network.

1. Before sending PHI in an internal email the appropriateness of the communication shall be considered. The criteria used to determine appropriateness of the communication are the same as apply to any communication of PHI.

2. Before sending PHI via internal email the email address and recipient should be verified.

3. Emails containing PHI should be deleted from the system after they are no longer required.

B. Email external to the Montgomery County network over the Internet.

1. The criteria used in determining the appropriateness of whether to send PHI via email over the internet are the same as determining whether to send internal email to other health plan employees or plan sponsor employees. Consideration should be given to the sensitivity of the information and the potential of inadvertent disclosure.

2. The email address of the recipient should be verified prior to sending the email.

3. Emails sent via the Internet shall be encrypted to reduce the risk of inadvertent disclosure of PHI.

4. Where possible, verification the recipient received the email should be obtained.

5. The email shall contain a notice that the email contains PHI.

XXI. CONVERSATIONS CONCERNING PHI.

A. Employees should conduct conversations concerning PHI in a manner that limits the risk of inadvertent disclosure of PHI through casual overhearing. Some conversations because of sensitive nature of the PHI or concerns by the member of inadvertent disclosure may only be possible in a private office or location.

B. Personnel initiating conversations or phone calls concerning PHI should be aware of their surroundings. For example a call concerning PHI made by a HR analyst/specialist to a business associate to discuss whether a diagnosis supports a certain medical procedure should not be made from the reception area with waiting area full.

C. Personnel initiating a call concerning PHI should be aware of the surroundings of the call recipient. Inquiry may need to be made as to whether the recipient can converse without danger of PHI being inadvertently disclosed to individuals in the immediate area of the call recipient.

D. When plan members initiate discussion of PHI with plan personnel, the plan personnel shall be cognizant of the potential for inadvertent disclosure of PHI when discussion takes place in reception or common areas of offices. Plan personnel shall move appropriate conversations to offices or other quieter locations that reduce the potential for inadvertent disclosure.

E. Leaving voice mail or forwarding voice mail containing PHI should be done with the same considerations as engaging in conversations concerning PHI.

XXII. TRAINING

A. Policy:

1. All personnel shall be trained in the requirements of protecting, using, and disclosing PHI.

B. Procedures:

1. All personnel shall be trained in the requirements and procedures necessary to implement the privacy policies contained herein as relates to their respective jobs.

2. Training shall consist of content sufficient to provide:

a. An overview of HIPAA and the Privacy Regulations

b. Detailed training on the policies and procedures relevant to the person's responsibilities.

C. The training materials will be maintained by the health plan on its web site or intranet for reference and review. In-service, refresher trainings will be conducted upon determination by the Privacy Officer that the policies, procedures, and laws have changed sufficiently to require further training or that compliance would be enhanced by additional training.

D. New employees and employees changing assignments will be required to undergo relevant privacy training as a condition of their assuming their responsibilities.

E. A log shall be maintained that tracks the initial training given to all employees, as well as updates and in-service refresher training modules.

XXIII. SANCTIONS AND MITIGATION

A. The health plan may discipline any employee who has violated these policies and procedures or the Privacy Regulations. Depending on the severity of the violation employee discipline may include verbal warning, letter of reprimand, retraining, suspension, or termination as appropriate. The Privacy Officer will document and maintain any sanctions that are imposed pursuant to the Retention of Documentation policy and procedures.

B. The health plan will *not* discipline any employee who:

1. Files a complaint with the Secretary of DHHS pursuant to the Privacy Regulations;

2. Testifies or assists in an investigation, compliance review, or hearing regarding the health plan's compliance with the Privacy Regulations; or

3. Opposes any act or practice that the employee believes, in good faith, is in violation of the law, and if the employee has not disclosed the PHI in violation of the Privacy Regulations and if the opposition is reasonable.

C. The health plan will take the appropriate and necessary steps to limit the harm of a use or disclosure by an employee or business associate in violation of these policies and procedures or the Privacy Regulations.

XXIV. RESERVATION OF RIGHT TO CHANGE POLICIES, PROCEDURES OR NOTICE

The health plan reserves the right to change these privacy policies and procedures and the Notice of Privacy Policies as the laws change or as circumstances dictate. When necessary, a revised Notice of Privacy Policies will be mailed to members.

1. Adopted by the Montgomery County Employee Benefit Plan April 7, 2003, effective April 14, 2003;

2. Revised April 11, 2005, effective April 15, 2005 – Security Provisions

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out payment, health care operations, and for other purposes that are permitted or required by law. It also sets out our legal obligations concerning your protected health information. Additionally, this Notice describes your rights to access and control your protected health information.

THIS NOTICE OF PRIVACY PRACTICES SHALL BECOME EFFECTIVE APRIL 14th, 2003.

Protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a health care provider, a health plan, your employer, or a health care clearinghouse and that relates to: (i) your past, present, or future physical or mental health or condition; (ii) the provision of health care to you; or (iii) the past, present, or future payment for the provision of health care to you.

If you have any questions or want additional information about the Notice or the policies and procedures described in the Notice, please contact the Director of Risk Management - 501 North Thompson Suite 202, Conroe, Texas 77301.

Our Responsibilities

We are required by law to maintain the privacy of your protected health information. We are obligated to provide you with a copy of this Notice of our legal duties and our privacy practices with respect to protected health information. And we must abide by the terms of this Notice. We reserve the right to change the provisions of our Notice and make the new provisions effective for all protected health information that we maintain. If we make a material change to our Notice, we will provide you a copy of the revised Notice.

Primary Uses and Disclosures of Protected Health Information

The following is a description of how we are most likely to use and/or disclose your protected health information.

Payment and Health Care Operations
We have the right to use and disclose your protected health information for all activities that are included within the definitions of "payment" and "health care operations" as set out in 45 C.F.R. § 164.501 (this provision is a part of what is known as "the HIPAA Privacy Regulations"). We have not listed in this Notice

all of the activities included within these definitions, so please refer to 45 C.F.R. § 164.501 for a complete list.

Section 1.01 Payment
We will use or disclose your protected health information to obtain premiums, to determine cost share, or otherwise fulfill our responsibilities for coverage and providing benefits as established under your member contract. For example, we may disclose your protected health information when a provider requests information regarding your eligibility for coverage under our health plan, or we may use your information to determine if a treatment that you received was medically necessary.

Section 1.02 Health Care Operations
We will use or disclose your protected health information to support our business functions. These functions include, but are not limited to: quality assessment and improvement, reviewing provider performance, licensing, business planning including using relevant information to obtain stop-loss coverage for the health plan, and business development. For example, we may use your information (i) to provide you with information about one of our disease management programs, (ii) to respond to a customer service inquiry from you, or, when certain conditions are met, (iii) to inform you about health-related benefits or services that may be of interest to you, (iv) to obtain quotes from potential business associates that provide services to the health plan.

Business Associates
We contract with individuals and entities (business associates) to perform various functions on our behalf or to provide certain types of services. Some of the functions they provide are administering claims, member service support, utilization management, subrogation, and pharmacy benefit management. To perform these functions or to provide the services, business associates will receive, create, maintain, use, or disclose protected health information, but only after we require the business associates to agree in writing to contract terms designed to appropriately safeguard your information.

Plan Sponsor
We may disclose your protected health information to Montgomery County, the plan sponsor of your group health plan.

Other Possible Uses and Disclosures of Protected Health Information

The following is a description of other possible ways in which we may (and are permitted to) use and/or disclose your protected health information.

Required by Law
We may use or disclose your protected health information to the extent that federal, state, or local law requires the use or disclosure. When used in this Notice, "required by law" is defined as it is in the HIPAA Privacy Regulations.

Public Health Activities
We may use or disclose your protected health information for public health activities that are permitted or required by law. For example, we may use or disclose information for the purpose of preventing or controlling disease, injury, or disability, or we may disclose such information to a public health authority authorized to receive reports of child abuse or neglect. We also may disclose protected health information, if directed by a public health authority, to a foreign government agency that is collaborating with the public health authority.

Health Oversight Activities
We may disclose your protected health information to a health oversight agency for activities authorized by law, such as audits; investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities. Oversight agencies seeking this information include government agencies that oversee: (i) the health care system, (ii) government benefit programs, (iii) other government regulatory programs, and (iv) compliance with civil rights laws.

Abuse or Neglect
We may disclose your protected health information to a government authority that is authorized by law to receive reports of abuse, neglect, or domestic violence. Additionally, as required by law, we may disclose to a governmental entity authorized to receive such information your information if we believe that you have been a victim of abuse, neglect, or domestic violence.

Legal Proceedings
We may disclose your protected health information: (1) in the course of any judicial or administrative proceeding; (2) in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized); and (3) in response to a subpoena, a discovery request, or other lawful process, once we have met all administrative requirements of the HIPAA Privacy Regulations.

Law Enforcement
Under certain conditions, we also may disclose your protected health information to law enforcement officials. Some of the reasons for such a disclosure may include, but not be limited to: (1) it is required by law or some other legal process; (2) it is necessary to locate or identify a suspect, fugitive, material witness, or missing person; and (3) it is necessary to provide evidence of a crime that occurred on our premises.

Coroners, Medical Examiners, Funeral Directors, and Organ Donation
We may disclose protected health information to a coroner or medical examiner for purposes of identifying a deceased person, determining a cause of death, or for the coroner or medical examiner to perform other duties authorized by law. We also may disclose, as authorized by law, information to funeral directors so that they may carry out their duties. Further, we may disclose protected health

information to organizations that handle organ, eye, or tissue donation and transplantation.

Research
We may disclose your protected health information to researchers when an institutional review board or privacy board has: (1) reviewed the research proposal and established protocols to ensure the privacy of the information and (2) approved the research.

To Prevent a Serious Threat to Health or Safety
Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We also may disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security, Protective Services
Under certain conditions, we may disclose your protected health information if you are, or were, Armed Forces personnel for activities deemed necessary by appropriate military command authorities. If you are a member of foreign military service, we may disclose, in certain circumstances, your information to the foreign military authority. We also may disclose your protected health information to authorized federal officials for conducting national security and intelligence activities, and for the protection of the President, other authorized persons, or heads of state.

Inmates
If you are an inmate of a correctional institution, we may disclose your protected health information to the correctional institution or to a law enforcement official for: (1) the institution to provide health care to you; (2) your health and safety and the health and safety of others; or (3) the safety and security of the correctional institution.

Workers' Compensation
We may disclose your protected health information to comply with workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.

Others Involved in Your Health Care
Unless you object, we may disclose your protected health information to a friend or family member that you have identified as being involved in your health care. We also may disclose your information to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status, and location. If you are not present or able to agree to these disclosures of your protected health information, then we may, using our professional judgment, determine whether the disclosure is in your best interest.

Required Disclosures of Your Protected Health Information

The following is a description of disclosures that we are required by law to make.

Disclosures to the Secretary of the U.S. Department of Health and Human Services
We are required to disclose your protected health information to the Secretary of the U.S. Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA Privacy Regulations.

Disclosures to You
We are required to disclose to you most of your protected health information in a "designated record set" when you request access to this information. Generally, a "designated record set" contains medical and billing records, as well as other records that are used to make decisions about your health care benefits. We also are required to provide, upon your request, an accounting of most disclosures of your protected health information that are for reasons other than payment and health care operations.

Other Uses and Disclosures of Your Protected Health Information

Other uses and disclosures of your protected health information that are not described above will be made only with your written authorization. If you provide us with such an authorization, you may revoke the authorization in writing, and this revocation will be effective for future uses and disclosures of protected health information. However, the revocation will not be effective for information that we already have used or disclosed, relying on the authorization.

YOUR RIGHTS

The following is a description of your rights with respect to your protected health information.

Right to Request a Restriction
You have the right to request a restriction on the protected health information we use or disclose about you for payment or health care operations.

We are not required to agree to any restriction that you may request. If we do agree to the restriction, we will comply with the restriction unless the information is needed to provide emergency treatment to you.

You may request a restriction by writing to **Privacy Officer**, 501 North Thompson Suite 202, Conroe, Texas 77301. In your request tell us: (1) the information whose disclosure you want to limit and (2) how you want to limit our use and/or disclosure of the information.

Right to Request Confidential Communications
If you believe that a disclosure of all or part of your protected health information may endanger you, you may request that we communicate with you regarding your information in an alternative manner or at an alternative location. For example, you can ask that we only contact you at your work address or via your work e-mail.

You may request a restriction by writing to Privacy Officer, 501 North Thompson Suite 202, Conroe, Texas 77301. In your request tell us: (1) the parts of your protected health information that you want us to communicate with you in an alternative manner or at an alternative location and (2) that the disclosure of all or part of the information in a manner inconsistent with your instructions would put you in danger.

Right to Inspect and Copy
You have the right to inspect and copy your protected health information that is contained in a "designated record set." Generally, a "designated record set" contains medical and billing records, as well as other records that are used to make decisions about your health care benefits. However, you may not inspect or copy psychotherapy notes or certain other information that may be contained in a designated record set.

To inspect and copy your protected health information that is contained in a designated record set, you must submit your request in writing to Privacy Officer, 501 North Thompson Suite 202, Conroe, Texas 77301. If you request a copy of the information, we may charge a fee for the costs of copying, mailing, or other supplies associated with your request.

We may deny your request to inspect and copy your protected health information in certain limited circumstances. If you are denied access to your information, you may request that the denial be reviewed. A licensed health care professional chosen by us will review your request and the denial. The person performing this review will not be the same one who denied your initial request. Under certain conditions, our denial will not be reviewable. If this event occurs, we will inform you in our denial that the decision is not reviewable.

Right to Request Amendment
If you believe that your protected health information is incorrect or incomplete, you may request that we amend your information. You may request that we amend your information by writing to Privacy Officer, 501 North Thompson Suite 202, Conroe, Texas 77301. Additionally, your request should include the reason the amendment is necessary.

In certain cases, we may deny your request for an amendment. For example, we may deny your request if the information you want to amend is not maintained by us, but by another entity. If we deny your request, you have the right to file a statement of disagreement with us. Your statement of disagreement will be linked

with the disputed information and all future disclosures of the disputed information will include your statement.

Right of an Accounting
You have a right to an accounting of most disclosures of your protected health information that are for reasons other than treatment, payment or health care operations. An accounting will include the date(s) of the disclosure, to whom we made the disclosure, a brief description of the information disclosed, and the purpose for the disclosure.

You may request an accounting by submitting your request in writing to Privacy Officer, 501 North Thompson Suite 202, Conroe, Texas 77301. Your request may be for disclosures made up to 6 years before the date of your request, but in no event, for disclosures made before April 14, 2003. The first list you request within a 12-month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at the time before any costs are incurred.

Right to a Paper Copy of This Notice
You have the right to a paper copy of this Notice, even if you have agreed to accept this Notice electronically.

Complaints

You may complain to us if you believe that we have violated your privacy rights. You may file a complaint with us by writing to Privacy Officer, 501North Thompson Suite 202, Conroe, Texas 77301. We have attached a complaint form for your convenience.

You also may file a complaint with the Secretary of the U.S. Department of Health and Human Services. Complaints filed directly with the Secretary must: (1) be in writing; (2) contain the name of the entity against which the complaint is lodged; (3) describe the relevant problems; and (4) be filed within 180 days of the time you became or should have become aware of the problem.

We will not penalize or in any other way retaliate against you for filing a complaint with us or with the Secretary.

Effective Date

This notice was published and becomes effective on April 14, 2003.
Revised April 15, 2005 to include Security Provisions.

Complaint Form to Privacy Officer

Privacy Officer:

Montgomery County

Privacy Officer
Montgomery County
501 North Thompson Suite 202
Conroe, TX 77301

Complainant Name:_____

Description of the subject of the complaint:

_____
_____
_____
_____

Check one or more of the following:

☐ Montgomery County Employee Health Plan used or disclosed protected health information to entities other than those permitted or required by HIPAA regulations.

☐ Montgomery County Employee Health Plan knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement and did not take reasonable steps to cure this breach or end the violation.

☐ Montgomery County Employee Health Plan is a hybrid entity and did not ensure that a health care component of the entity complied with applicable requirements, such as disclosure of protected health information to other entities that would be prohibited from having this information if the health care component and the other component were separate and distinct legal entities.

☐ Montgomery County Employee Health Plan did not obtain the individual's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.

☐ Montgomery County Employee Health Plan did not obtain authorization for any use or disclosure of psychotherapy notes (exception – to carry out treatment, payment or health care operations consistent with consent requirements).

☐ Montgomery County Employee Health Plan did not inform in advance of the use or disclosure of protected health information and did not allow opportunity to orally agree or prohibit or restrict disclosure.

☐ Other _____

_____

Describe the acts or omissions believed to be in violation of the applicable requirements, standards, and implementation specifications of H.I.P.A.A. regulations. Include dates in description.

Description of acts or omissions supporting the complaint:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Signature of complainant: _____Date _____

Print name of complainant: _____

Note: You also have the right to file a complaint with the Secretary of Health and Human Services within 180 days of when the you knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. No retaliatory action can be filed against you for filing this complaint. **No retribution or negative action will be taken or tolerated because a member files a complaint with the health plan or the Secretary.**

OCR HEALTH INFORMATION PRIVACY COMPLAINT FORM

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS (OCR)

HEALTH INFORMATION PRIVACY COMPLAINT

If you gave questions about this form, call OCR (toll-free) at:
1-800-368-1019 (any language) or 1-800-537-7697 (TDD)

YOUR FIRST NAME		YOUR LAST NAME
HOME PHONE ( )		WORK PHONE ( )
STREET ADDRESS		CITY
STATE	ZIP	E-MAIL ADDRESS (If available)

Are you filing this complaint for someone else? ☐ Yes ☐ No
If Yes, whose health information privacy rights do you believe were violated?
FIRST NAME LAST NAME

Who (or what agency or organization, e.g., provider, health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?
PERSON/ AGENCY/ ORGANIZATION

STREET ADDRESS		CITY
STATE	ZIP	PHONE ( )

When do you believe that the violation of health information privacy rights occurred?
LIST DATE(S)

Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the privacy rule otherwise was violated? Please be as specific as possible. (Attach additional pages as needed)

Please sign and date this complaint. SIGNATURE	DATE

Filing a complaint with OCR is voluntary. However, without the information requested above, OCR may be unable to proceed with your complaint. We collect this information under authority of the Privacy Rule issued pursuant to the Health Insurance Portability and Accountability Act of 1996. We will use the information you provide to determine if we have jurisdiction and, if so, how we will process your complaint. Information submitted on this form is treated confidentially and is protected under the provisions of the Privacy Act of 1974. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, for internal systems operations, or for routine uses, which include disclosure of information outside the Department for purposes associated with health information privacy compliance and as permitted by law. It is illegal for a covered entity to intimidate, threaten, coerce, discriminate or retaliate against you for filing this complaint or for taking any other action to enforce your rights under the Privacy Rule. You are not required to use this form. You also may write a letter or submit a complaint electronically with the same information. To submit an electronic complaint, go to our web site at: www.hhs.gov/ocr/privacyhowtofile.html. To mail a complaint see reverse page for OCR Regional addresses.

(The remaining information on this form is optional. Failure to answer these voluntary questions will not affect OCR's decision to process your complaint.)

Do you need special accommodations for us to communicate with you about this complaint (check all that apply)?

☐ Braille ☐ Large Print ☐ Cassette tape ☐ Computer diskette ☐ Electronic mail ☐ TDD
☐ Sign language interpreter (specify language): _____
☐ Foreign language interpreter (specify language): _____ ☐ Other: _____

If we cannot reach you directly, is there someone we can contact to help us reach you?

FIRST NAME		LAST NAME
HOME PHONE ( )		WORK PHONE ( )
STREET ADDRESS		CITY
STATE	ZIP	E-MAIL ADDRESS (If available)

Have you filed your complaint anywhere else? If so, please provide the following. (Attach additional pages as needed.)

PERSON / AGENCY / ORGANIZATION / COURT NAME(S)	
DATE(S) FILED	CASE NUMBER(S)

To help us better serve the public, please provide the following information for the person you believe had their health information privacy rights violated (you or the person on whose behalf you are filing).

ETHNICITY (select one)
☐ Hispanic or Latino
☐ Not Hispanic or Latino

RACE (select one or more)
☐ American Indian or Alaska Native ☐ Asian ☐ Native Hawaiian or Other Pacific Islander
☐ Black or African American ☐ White ☐ Other (specify): _____

PRIMARY LANGUAGE SPOKEN (if other than English)

HOW DID YOU LEARN ABOUT THE OFFICE FOR CIVIL RIGHTS?

_____/_____

To mail a complaint, please type or print, and return completed complaint to the OCR Regional Address based on the region where the alleged violation took place.

Region I – CT, ME, MA NH, RI, VT Office for Civil Rights Department of Health & Human Services JFK Federal Building – Room 1875 Boston, MA 02203 (617) 565-1340; (617) 565-1343 (TDD) (617) 565-3809 FAX	**Region V – IL, IN, MI, MN, OH, WI** Office for Civil Rights Department of Health & Human Services 233 N. Michigan Ave. – Suite 240 Chicago, IL 60601 (312) 886-2359; (312) 353-5693 (TDD) (312) 886-1807 FAX	**Region IX – AZ, CA, HI, NV, AS, GU** **The U.S. Affiliated Pacific Island Jurisdictions** Office for Civil Rights Department of Health & Human Services 50 United Nations Plaza – Room 322 San Francisco, CA 94102 (415) 437-8310; (415) 437-8311 (TDD) (415) 437-8329 FAX
Region II – NJ, NY, PR, VI Office for Civil Rights Department of Health & Human Services 26 Federal Plaza – Suite 3313 New York, NY 10278 (212) 264-3313; (212) 264-2355 (TDD) (212) 264-3039 FAX	**Region VI – AR, LA, NM, OK, TX** Office for Civil Rights Department of Health & Human Services 1301 Young Street – Suite 1169 Dallas, TX 75202 (214) 767-4056; (214) 767-8940 (TDD) (214) 767-0432 FAX	**Region X – AK, ID, OR, WA** Office for Civil Rights Department of Health & Human Services 2201 Sixth Avenue – Mail Stop RX-11 Seattle, WA 98121 (206) 615-2290; (206) 615-2296 (TDD) (206) 615-2297 FAX
Region III – DE, DC, MD, PA, VA, WV Office for Civil Rights Department of Health & Human Services 150 S. Independence Mall West – Suite 372 Philadelphia, PA 19106-3499 (215) 861-4441; (215) 861-4440 (TDD) (215) 861-4431 FAX	**Region VII – IA, KS, MO, NE** Office for Civil Rights Department of Health & Human Services 601 East 12th Street – Room 248 Kansas City, MO 64106 (816) 426-7278; (816) 426-7065 (TDD) (816) 426-3686 FAX	
Region IV – AL, FL, GA, KY MS, NC, SC, TN Office for Civil Rights Department of Health & Human Services 61 Forsyth Street, SW. – Suite 3B70 Atlanta, GA 30323 (404) 562-7886; (404) 331-2867 (TDD) (404)562-7881 FAX	**Region VIII–CO, MT, ND, SD, UT, WY** Office for Civil Rights Department of Health & Human Services 1961 Stout Street – Room 1426 Denver, CO 80294 (303) 844-2024; ((303) 844-3439 (TDD) (303) 844-2025 FAX	

Burden Statement

Public reporting burden for the collection of information on this complaint form is estimated to average 45 minutes per response, including the time for reviewing instructions, gathering the data needed and entering and reviewing the information on the completed complaint form. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: HHS/OS reports Clearance Officer, Office of Information Resources Management, 200 Independence Ave. S.W., Room 531H, Washington, D.C. 20201

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN
INDIVIDUAL REQUEST TO INSPECT HEALTH INFORMATION

I request to review health information held about me in the Montgomery County Employee Benefit Plan's "designated record set" in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A "designated record set" includes information such as medical records; billing records; enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used to make decisions about individuals.

I understand that the group health plan has 30 days to respond to this request, and that if someone else holds the information or it is off-site, the response time is 60 days.

I request that the information be provided in the following format: **(circle one) paper electronic**

I agree that the group health plan may provide a summary of the health information instead of allowing me to review the information.

I agree to pay any fees for copying or summarizing my health information. Fees will be reasonable and cost-based, and include only the cost of copying, postage, and preparation of a summary (if I agree to a summary).

I understand that this request does not apply to certain health information, including: (1) information that is not held in the designated record set; (2) psychotherapy notes; (3) information compiled in reasonable anticipation of or for litigation; and (4) other information not subject to the right to access information under HIPAA.

Signature: _____ **Date:** _____

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN'S
RESPONSE TO INSPECTION REQUEST

☐ **Grant**

Your request to access you health information has been granted: Access will be provided at

_____

☐ **Need for Extension of Time**

The Montgomery County Employee Benefit Plan received your request to access health information on _____. The Montgomery County Employee Benefit Plan has evaluated your request to access health information. A delay in providing the information is necessary for the following reason:_____

The Montgomery County Employee Benefit Plan will respond to your request by: _____
(The designated date is no later than 60 days from the date of the request.)

☐ **Denial of Access**

The Montgomery County Employee Benefit Plan received your request to access health information on: _____. Your request is denied for the following reason:

_____

_____

You may file a complaint regarding this decision with the Montgomery County Employee Benefit Plan or the U.S. Department of Health and Human Services. If you file a complaint with Montgomery County Employee Benefit Plan, please file it in writing with the following person:

Privacy Officer, Montgomery County
501 N. Thompson, Suite 202
Conroe, TX 77301

In certain cases you are entitled to appeal the denial of access. You are entitled to an appeal if access was denied because in the opinion of a licensed health care professional, granting access is likely to endanger the life or physical safety of you or another person. If you appeal, your appeal will be reviewed by a licensed health care professional designated by the plan who did not participate in the original decision. The appeal and notice of the appeal will be conducted promptly.

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN
INDIVIDUAL REQUEST TO CORRECT OR AMEND A RECORD

I request the Montgomery County Employee Benefit Plan to amend the protected health information in its designated record set.

Specific Statement of Amendment Request:

_____

_____

Specific Reason for Amendment Request:

_____

_____

I understand that if the protected health information was not created by the Montgomery County Employee Benefit Plan, the group health plan is not required to honor my request. For example, if the information I wish to amend is in a medical report created by my physician, I must ask the physician – not the Montgomery County Employee Benefit Plan – to amend the report. I also understand that if the information is not available for my inspection, is not part of the Montgomery County Employee Benefit Plan's designated record set or is already accurate and complete, I cannot amend the information.

I understand that the Montgomery County Employee Benefit Plan will respond to my request within 60 days.

Signature: _____ Date: _____

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN'S
RESPONSE TO AMENDMENT OR CORRECTION

☐ **Grant**

Your request to amend or correct your health information has been granted. The Montgomery County Employee Benefit Plan will make an appropriate amendment to the designated record set.

You must provide the Montgomery County Employee Benefit Plan with the names of any persons to which you wish to provide the amended information. The Montgomery County Employee Benefit Plan then will make reasonable efforts to inform these individuals – and persons that the Montgomery County Employee Benefit Plan knows may have relied or could rely on the information – of the amendment within a reasonable time.

☐ **Need for Extension of Time**

The Montgomery County Employee Benefit Plan received your request to amend health information on: _____. Your request is denied for the following reason _____

_____

The Montgomery County Employee Benefit Plan will respond to your request by:

_____

(The designated date is no later than 60 days from the date of the request.)

☐ **Denial of Amendment**

The Montgomery County Employee Benefit Plan received your request to amend health information on _____

Your request is denied for the following reason:_____

_____

Statement of Disagreement

Your have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement must be limited to two single-sided 8-1/2 x 11 pages. The statement of disagreement should be filed within 60 days of this notice with the following office, **Risk Management, Montgomery County**. The Montgomery County Employee Benefit Plan has a right to prepare a rebuttal statement to your statement of disagreement. If it does so, you will receive a copy.

If you do not submit a statement of disagreement, you may request that the Montgomery County Employee Benefit Plan provide your request for amendment and this denial of amendment with any future disclosure of protected health information that is the subject of this request.

You may file a complaint regarding this decision with the Montgomery County Employee Benefit Plan or the U.S. Department of Health and Human Services. If you file a complaint with the Montgomery County Employee Benefit Plan, please file it in writing with the following person:

Privacy Officer, Montgomery County
Risk Management Department
501 N. Thompson, Suite 202
Conroe, TX 77301
Phone: 936-760-6935

MONTGOMERY COUNTY EMPLOYEE BENEFIT PLAN
INDIVIDUAL REQUEST NOT TO USE OR DISCLOSE HEALTH INFORMATION

I understand that the Montgomery County Employee Benefit Plan may use and disclose protected health information about me for purposes of health care treatment, payment and health care operations without my consent. I request to restrict use and disclosure of protected health information concerning health care treatment, payment or health care operations about me by the Montgomery County Employee Benefit Plan in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Group Health Plan Not Required to Agree

I understand that the Montgomery County Employee Benefit Plan is not required to agree to this restriction.

Termination of Restriction

I understand that if the Montgomery County Employee Benefit Plan agrees to this restriction, either the Plan or I may terminate this restriction at any time. The termination of the restriction is only effective for future uses and disclosures.

Emergency Treatment Exception

I understand that if protected health information must be used or disclosed to provide emergency treatment for me, then this restriction is void.

Questionnaire

Requestor: Please complete all of the following questions. If the question is not applicable, mark N/A on the answer line.

1. I request the following information be restricted:

_____

_____

2. I request that use and disclosure of the above described information be restricted in the following manner:

_____

_____

3. I request that my protected health information not be disclosed to the following individuals or entities:

_____

_____

I understand that if a restriction is not specifically listed above and agreed to in writing by the Montgomery County Employee Benefit Plan, it will not be effective.

Signature: _____ **Date:** _____

Risk Management

501 North Thompson, Suite 202
Conroe, Texas 77301
Phone 936/760-6935 Fax 936/760-6916
H.I.P.A.A. Fax 936/538-8169

To: Montgomery County Employee Benefit Plan H.I.P.A.A. Privacy Officer

I, _____, ☐ employee or ☐ participating eligible dependent, authorize Montgomery County Risk Management employees to access the following benefits,

☐ Medical ☐ Vision ☐ Dental ☐ Group life Insurance ☐AD&D

in regards to types of coverage and questions relating to plan document provisions and claims for the following dates of service: _____

Medical information/Explanation of Benefits are not filed in the Risk Management Department. After resolution, medical information will be shredded. Be sure to keep your original paperwork for your files.

Doctors: _____
Facilities: _____

☐ I also give my permission to discuss the information with any of the listed above with the following individuals:

_____Relationship _____
_____Relationship _____
_____Relationship _____

Employee or a participating eligible Dependent

_____Social Security # _____
Print Name

_____Date _____
Signature

Witnessed by _____Date _____

Print Name _____

1) Right to revoke: I understand that I have the right to revoke this authorization at any time by notifying Montgomery County Employee Benefit Plan in writing at the Risk Management Department, 501 N. Thompson, Suite 202; Conroe, TX 77301. I understand that the revocation is only effective after it is received and logged by the Risk Management Department on behalf of Montgomery County Employee Benefit Plan. **2**) I understand that after this information is disclosed, federal law might not protect it and the recipient might redisclose it. **3)** I understand that I am entitled to receive a copy of the authorization. **4**) I understand that this authorization will expire when my participation under the Montgomery County Employee Benefit Plan ends.