

HIPAA POLICIES & PROCEDURES AND ADMINISTRATIVE FORMS TABLE OF CONTENTS

1. HIPAA Privacy Policies & Procedures Overview (Policy & Procedure)
2. HIPAA Privacy Officer (Policy & Procedure)
3. Notice of Privacy Practices (Policy & Procedure)
 - a. Notice of Privacy Practice for Organized Health Care Arrangement (Administrative Form)
4. Use of Disclosure of PHI for TPO Purposes (Policy & Procedure)
5. Minimum Necessary Standard (Policy & Procedure)
6. Individual's Rights to Access and Copy PHI (Policy & Procedure)
 - a. Request to Access Own PHI (Administrative Form)
 - b. Grant of Request to Access Own PHI (Administrative Form)
 - c. Notification of Additional Time to Respond to Access to Own PHI (Administrative Form)
 - d. Denial of Request to Access Own PHI (Administrative Form)
 - e. Access Request Tracking Log (Administrative Form)
7. Amendment of PHI (Policy & Procedure)
 - a. Request for Amendment of PHI Request (Administrative Form)
 - b. Grant of Amendment of PHI Request (Administrative Form)
 - c. Notification of Additional Time to Respond to Amendment of PHI (Administrative Form)
 - d. Denial of Request for Amendment of PHI (Administrative Form)
 - e. Notice to Others of Amendment of PHI (Administrative Form)
 - f. Requestor's List of Person's or Entities to Be Notified of Amendment (Administrative Form)
 - g. Amendment Request Tracking Log (Administrative Form)
8. Accounting of Disclosures of PHI (Policy & Procedure)
 - a. Request for An Accounting of Disclosures (Administrative Form)
 - b. Accounting of Disclosures of PHI (Administrative Form)
 - c. Notification of Additional Time to Respond to Accounting Request (Administrative Form)

- d. Notification of Charges for Second Request in 12 Month Period (Administrative Form)
 - e. Accounting Request Tracking Log (Administrative Form)
 - f. Disclosure Tracking Log (Administrative Form)
9. Verification Prior to Disclosure of PHI (Policy & Procedure)
 - a. Disclosure Tracking Log (Administrative Form)
 10. Individual Requested Restrictions of Use or Disclosure of PHI (Policy & Procedure)
 - a. Request to Restrict Certain Uses and Disclosures (Administrative Form)
 - b. Response to Request to Restrict Certain Uses and Disclosures (Administrative Form)
 11. Individual Requested Restrictions on Confidential Communications (Policy & Procedure)
 - a. Request for Confidential Communications (Administrative Form)
 - b. Restricted Uses and Confidential Communication Request Tracking Log (Administrative Form)
 12. Privacy Complaint Procedure (Policy & Procedure)
 - a. Privacy Complaint Form (Administrative Form)
 - b. Response to Privacy Complaint (Administrative Form)
 - c. Complaint Tracking Log (Administrative Form)
 13. Authorization for Use or Disclosure of PHI (Policy & Procedure)
 - a. Authorization for Use or Disclosure (Administrative Form)
 14. Revocation of an Authorization (Policy & Procedure)
 - a. Revocation by Subject of Protected Health Information (Administrative Form)
 15. Business Associates and Business Associate Agreements (Policy & Procedure)
 16. Retention of PHI Documentation (Policy & Procedure)
 17. HIPAA Privacy Training Program (Policy & Procedure)
 - a. Acknowledgment of Training Attendance (Administrative Form)
 18. Personal Representative (Policy & Procedure)
 - a. Designation of Personal Representative (Administrative Form)
 19. Coordination with Other Laws (Policy & Procedure)
 20. Disclosures to Plan Sponsor (Policy & Procedure)
 21. Duty to Mitigate (Policy & Procedure)
 22. Discipline Policy (Policy & Procedure)

23. Administrative Safeguards (Policy & Procedure)
 1. Computer Terminals/Workstations (Policy & Procedure)
 2. Electronic Mail System (E-mail) (Policy & Procedure)
 3. Facsimile Machines (Policy & Procedure)
 4. Copy Machines (Policy & Procedure)
 5. Mail – Internal and External (Policy & Procedure)
 6. Storage of Documents (Policy & Procedure)

HIPAA Privacy Policies and Procedures Overview

Policy Statement

HIPAA requires covered entities to have policies and procedures reflecting HIPAA's privacy mandates. The Health Plan, as a covered entity, has developed administrative policies and procedures reflecting the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy regulations.

Policy Interpretation and Implementation

HIPAA Policies and Procedures

1. HIPAA requires covered entities to have policies and procedures to ensure compliance with HIPAA's regulations. A health plan is a "covered entity" under HIPAA. Consequently, the Health Plan is responsible for the research, development, implementation, monitoring and maintenance of the Health Plan's HIPAA privacy policies and procedures.

Health Plan

2. HIPAA defines a "health plan" as an individual or group health plan that provides or pays the cost of medical care, including, but not limited to, employee welfare benefit plans covered by ERISA, health insurers, HMOs, group health plans, and many public benefit programs (Medicaid, Medicare, etc.).

Revisions to HIPAA Policies and Procedures

3. The Health Plan's HIPAA privacy policies and procedures may be revised at any time, in order to comply or enhance compliance with HIPAA.

Distribution of Revisions to HIPAA Policies and Procedures

4. Any revisions to the Health Plan's HIPAA privacy policies and procedures will be distributed to individual's family members, representatives, employees, business associates, etc., within five (5) working days of the release of such revisions.

Policy Inquiries

5. Inquiries relative to HIPAA policies and procedures should be directed to the HIPAA Privacy Officer.

Specific Policies and Procedures

6. The Health Plan's specific policies and procedures have been created in order to satisfy HIPAA's requirements.

Organized Health Care Arrangement (OHCA)

7. HIPAA recognizes Organized Health Care Arrangements (OHCAs). An OHCA can exist when an employer sponsors more than one health plan that is a covered entity. Being part of an OHCA allows the covered entities to satisfy the HIPAA privacy requirements together, as if they are a single covered entity. The following covered entities are designated as an OHCA:

City of Mendota Heights

For purposes of these HIPAA privacy policies and procedures, "Health Plan" means the OHCA designated above.

Third Party Service Providers

8. Nothing precludes the Health Plan from contracting with a third party service for assistance in complying with the Health Plan's HIPAA privacy policies and procedures.

Other Laws

9. In addition to HIPAA, covered entities may be subject to other laws that address the privacy of health information, including, but not limited to, the Minnesota Data Practices Act. HIPAA establishes a floor – the minimum requirements with which a covered entity must comply. To the extent the requirements of any other law provide more protection to the subject of the health information, those requirements will apply.

Record Retention

10. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

11. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. If you have a question or concern about your HIPAA rights contact the HIPAA Privacy Officer at 651-452-1850.

Violations

12. Violations of this policy will be subject to discipline.

Effective Date

13. April 14, 2004

References:

45 C.F.R. § 164.501

HIPAA Privacy Officer

Policy Statement

A HIPAA Privacy Officer has been designated by this Health Plan to be responsible for the development and implementation of this Health Plan's HIPAA policies and procedures.

Policy Interpretation and Implementation

Appointment of HIPAA Privacy Officer

1. The Health Plan has appointed the Human Resources/Communications Coordinator, as the Health Plan's HIPAA Privacy Officer.

HIPAA Privacy Officer's Responsibilities

2. The HIPAA Privacy Officer's responsibilities include:
 - a. Assisting management in the development, implementation, and updating of the Health Plan's HIPAA policies and procedures;
 - b. Performing periodic privacy risk assessments;
 - c. Development of security procedures and guidelines for the protection of the Health Plan's information systems;
 - d. Assisting management in the assigning of passwords and user identification codes for access to protected health information (PHI) by authorized users;
 - e. Receiving complaints concerning the Health Plan's HIPAA policies and procedures;
 - f. Receiving complaints concerning the Health Plan's compliance with its established policies and procedures;
 - g. Maintaining a complaint tracking log;
 - h. Assisting in obtaining use and disclosure of PHI authorizations;
 - i. Assisting in the development of training materials and training to ensure that relevant staff are well trained in matters relating to the use and disclosure of protected health information (PHI);
 - j. Providing staff, individuals, business associates, government agencies etc., with information relative to the Health Plan's HIPAA policies and procedures; and
 - k. Working with the Health Plan's legal counsel on matters relative to HIPAA.

Delegation

3. The HIPAA Privacy Officer may delegate certain job functions to be performed by other individuals; however, the ultimate responsibility for compliance with HIPAA

remains with the HIPAA Privacy Officer.

Record Retention

4. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

5. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

6. Violations of this policy will be subject to discipline.

Effective Date

7. April 14, 2004.

References:

45 C.F.R. § 164.530(a)

Notice of Privacy Practices

Policy Statement

Each individual that is the subject of Protected Health Information (PHI) must receive a Notice of Privacy Practices (NPP) describing (1) the uses and disclosures of his/her PHI that may be made by or on behalf of the Health Plan, (2) the individual's rights, and (3) the Health Plan's legal duties with respect to the individual's PHI.

Policy Interpretation and Implementation

Issue of NPP

1. Individuals who are covered under the Health Plan will be provided with a copy of the Health Plan's NPP;

Content of NPP

2. NPPs must be prepared in easy to read language and contain, as a minimum, the following elements:
 - a. A statement indicating how medical information about the individual may be used and disclosed and how the individual can obtain access to such information;
 - b. A description, including at least one example, of the types of uses and disclosures that the Health Plan is permitted to make for purposes of treatment, payment and healthcare operations, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;
 - c. A description of each of the other purposes for which the Health Plan is permitted or required to use or disclose PHI without the individual's consent or authorization, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;
 - d. A statement that other uses or disclosures will be made only with the individual's written authorization, and that the authorization may be revoked in accordance with the policy on authorization;
 - e. A statement of the individual's rights with respect to his/her PHI, and a brief description of how the individual may exercise those rights, including:
 - i. The right to request restrictions on certain uses/disclosures of PHI, and the fact that the Health Plan does not have to agree to such restrictions;
 - ii. The right to receive confidential communications of PHI;
 - iii. The right to inspect and copy PHI;

- iv. The right to amend PHI;
 - v. The right to receive an accounting of disclosures of PHI; and
 - vi. The right to receive a paper copy of the privacy notice.
- f. A statement of the Health Plan's duties with respect to PHI, including statements:
- i. That the Health Plan is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices;
 - ii. That the Health Plan is required to abide by the terms of its current effective privacy notice; and
 - iii. That the Health Plan reserves the right to change the terms of the notice and make a new notice provision effective for all PHI maintained, along with a description of how the Health Plan will provide individuals with the revised notice.
- g. A statement that individuals may complain to the Health Plan and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual will not be retaliated against for filing a complaint;
- h. The name, or title, and telephone number of the Health Plan's HIPAA Privacy Officer to contact for further information;
- i. The name, telephone number and address of the person designated by the Health Plan to receive complaints regarding the Health Plan's privacy practices; and
- j. The effective date of the NPP, which may not be earlier than the date printed or published.

Distribution of NPP

3. The Health Plan will distribute the NPPs at the times specified below:
- a. On the Health Plan's initial compliance date;
 - b. At the time of enrollment in the Health Plan for new enrollees; and
 - c. Within sixty (60) days of a material revision of the NPP to individuals covered by the Health Plan.
4. The NPP will be distributed no less frequently than once every three (3) years.

5. The NPP will be delivered by first class U.S. Mail to the address of record on file with the Health Plan. The NPP will be addressed to the individual, spouse and all dependents covered by the Health Plan.

Posting of NPP

6. A copy of the NPP will be posted on the web page, if one, of the employer sponsoring the Health Plan. The HIPAA Privacy Officer is responsible for prompt distribution of changes to the privacy notice.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. April 14, 2004.

References:

45 C.F.R. § 164.520

City of Mendota Heights ORGANIZED HEALTH CARE ARRANGEMENT NOTICE OF PRIVACY PRACTICES

Effective April 14, 2004

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.

If you have any questions about this notice, please contact the **Privacy Officer**:

Human Resources/Communications Coordinator
City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118
651-452-1850
cityhall@mendota-heights.com

Who Will Follow This Notice

This notice describes the medical information practices of the City of Mendota Heights organized health care arrangement ("OHCA") and third parties that assists in the administration of OHCA Plan.

For purposes of HIPAA and this notice, the OHCA includes the following:

- Health Reimbursement Account
- Employee Assistance Program
- Medical Insurance
- Dental Insurance

Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. This notice applies to all of the medical records maintained by an OHCA Plan. Your personal doctor or health care provider may have different policies or notices regarding the doctor's use and disclosure of your medical information created in the doctor's office or clinic.

This notice tells you about the ways in which we may use and disclose medical information about you. It also describes our obligations and your rights regarding the use and disclosure of medical information.

We are required by law to:

- make sure that medical information that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- follow the terms of the notice that are currently in effect.

How We May Use and Disclose Medical Information About You

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures, we will explain what we mean and present some examples. These

examples are not exhaustive. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Please note: In most instances, how information is used and disclosed has not changed. The descriptions reflect how the Health Plans that make up the OHCA have traditionally operated.

For Treatment (as described in applicable regulations). We may use or disclose medical information about you to facilitate medical treatment or services by providers. We may disclose medical information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you.

For Payment (as described in applicable regulations). We may use and disclose medical information about you to determine eligibility for benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under an OHCA Plan, or to coordinate OHCA Plan coverage. For example, we may tell your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary or to determine whether the OHCA Plan covers the treatment. We may also share medical information with a utilization review or pre-certification service provider. Likewise, we may share medical information with another entity to assist with the adjudication (legal actions) or subrogation (third party reimbursements) of health claims or to another health plan to coordinate benefit payments.

For Health Care Operations (as described in applicable regulations). We may use and disclose medical information about you for other OHCA Plan operations. These uses and disclosures are necessary to run the OHCA Plan. For example, we may use medical information in connection with: conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to OHCA Plan coverage; submitting claims for stop-loss (or excess loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as cost management; and business management and general OHCA Plan administrative activities.

As Required By Law. We will disclose medical information about you when required to do so by federal, state or local law. For example, we may disclose medical information when required by a court order or subpoena.

To Avert a Serious Threat to Health or Safety. An OHCA may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. However disclosure would be limited to someone able to help prevent the threat.

Special Situations

Disclosure to Health Plan Sponsor. Information may be disclosed to another health plan for purposes of facilitating claims payments under that plan. In addition, medical information may be disclosed to City of Mendota Heights personnel solely for administering benefits under the OHCA Plan.

Organ and Tissue Donation. If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military and Veterans. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation. We may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose medical information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe an individual has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may release medical information if asked to do so by a law enforcement official:

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct; and
- in emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

Coroners, Medical Examiners and Funeral Directors. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the hospital to funeral directors as necessary to carry out their duties.

National Security and Intelligence Activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Your Rights Regarding Medical Information About You

You have the following rights regarding medical information we maintain about you:

Right to Inspect and Copy. You have the right to inspect and copy medical information that may be used to make decisions about your OHCA Plan benefits. To inspect and copy the medical information that may be used to make decisions about you, you must submit your request in writing to the Privacy Officer. 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 in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed.

Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the OHCA Plan.

To request an amendment, your request must be made in writing and submitted to the Privacy Officer. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- is not part of the medical information kept by or for the OHCA Plan;
- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information which you would be permitted to inspect and copy; or is accurate and complete.

Right to an Accounting of Disclosures. You have the right to request an "accounting of disclosures" where such disclosure was made for any purpose other than treatment, payment, or health care operations.

To request this list of accounting of disclosures, you must submit your request in writing to Privacy Officer. Your request must state a time period which may not be longer than six years and may not include dates before April, 2004. Your request should indicate in what form you want the list (for example, paper or electronic). 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 that time before any costs are incurred.

Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. We are not required to agree to your request.

To request restrictions, you must make your request in writing to the Privacy Officer. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you

can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to the Privacy Officer. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice.

You may obtain a copy of this notice at our website, www.mendota-heights.com. To obtain a paper copy of this notice, contact the Privacy Officer.

Changes to This Notice

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice on the OHCA Plan website. The notice will contain on the first page, in the top right hand corner, the effective date.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with the OHCA Plan or with the Secretary of the Department of Health and Human Services. To file a complaint with the OHCA Plan, contact the Privacy Officer. All complaints must be submitted in writing.

You will not be penalized for filing a complaint.

Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this notice or the other applicable laws will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Use or Disclosure of PHI

Policy Statement

In order for the Health Plan to use or disclose (including obtaining) protected health information (PHI), the use or disclosure must either (1) fall under the enumerated uses and disclosures allowed without an individual authorization, or (2) the Health Plan must obtain an individual authorization.

Policy Interpretation and Implementation

Definition of PHI

1. *Protected Health Information (PHI)* means individually identifiable information relating to:
 - a. The past, present or future physical or mental health or condition of an individual;
 - b. The provision of health care to an individual;
 - c. The past, present or future payment for health care provided to an individual.

Use and Disclosure not Requiring an Individual Authorization

2. PHI may only be used or disclosed without an individual authorization for treatment, payment, or health care operations (TPO). These purposes include:
 - a. The Health Plan may use or disclose PHI for its own TPO;
 - b. The Health Plan may disclose PHI to another covered entity for the payment activities of that entity;
 - c. The Health Plan may disclose PHI to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI, the PHI pertains to such relationship, and the disclosure is:
 - i. For health care operations regarding conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not include treatment, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, credentialing activities; or
 - ii. For the purpose of health care fraud and abuse detection or compliance;

- d. If the Health Plan participates in an organized health care arrangement (OHCA), it may disclose PHI about an individual to another covered entity that participates in the OHCA for any health care operations activities of the OHCA.

Nothing in paragraph 2 prevents the Health Plan from obtaining an individual authorization for use and disclosure of PHI for TPO purposes.

Definition of TPO

- 3. *Treatment, Payment and Health Care Operations (TPO)* includes all of the following:
 - a. *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual or referral of an individual to another provider for health care.
 - b. *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
 - c. *Health Care Operations* includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

Use and Disclosure for Public Policy Reasons

4. PHI may be used or disclosed without an individual authorization as required by law and for other public policy reasons when specific requirements are met. The situations in which PHI may be disclosed for public policy reasons include, but are not limited to, situations involving:
 - a. serious threats to health or safety;
 - b. disclosures to health plan sponsor;
 - c. organ and tissue donation;
 - d. military and veterans;
 - e. workers' compensation;
 - f. public health risks;
 - g. health oversight activities;
 - h. lawsuits and disputes;
 - i. law enforcement;
 - j. coroners, medical examiners and funeral directors;
 - k. national security and intelligence activities; and
 - l. inmates.

Use and Disclosure Requiring an Individual Authorization

5. An individual authorization is required for any use or disclosure of PHI that is not specifically allowed by the HIPAA privacy regulations (without the individual authorization). These uses and disclosures include, but are not limited to:
 - a. Use or disclosure of psychotherapy notes;
 - b. Use or disclosure of PHI for purposes of marketing, except if the communication is in the form of:
 - i. Face-to-face communication made by the Health Plan to an individual; or
 - ii. A promotional gift of nominal value provided by the Health Plan.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. April 14, 2004.

References:

45 C.F.R. §§164.506, 164.508, 164.512

Minimum Necessary Standard

Policy Statement

Whenever practical/feasible, the Health Plan will make reasonable efforts to limit use and disclosure of protected health information (PHI) to the minimum necessary to accomplish the appropriate intended purpose.

Policy Interpretation and Implementation

Minimum Necessary Standard

1. When using, disclosing or requesting PHI, the Health Plan shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose.

Access to PHI

2. The Health Plan requires relevant staff to have access only to the minimum necessary PHI required by their job functions.

It is the responsibility of the HIPAA Privacy Officer to limit the access of relevant staff to only the minimum necessary PHI required by their job function. The HIPAA Privacy Officer may delegate certain job functions to be performed by other individuals; however, the ultimate responsibility for compliance with HIPAA remains with the HIPAA Privacy Officer.

Where Minimum Necessary Standard Does Not Apply

3. Limiting use, disclosure or request of PHI to the minimum necessary does NOT apply in the following situations:
 - a. Disclosures or requests by a health care provider for treatment;
 - b. Uses or disclosures made to the individual or requested and authorized by the individual;
 - c. Disclosures made to the Secretary of Health and Human Services (HHS) or to the Office of Civil Rights (OCR);
 - d. Uses or disclosures required by law; and/or
 - e. Uses or disclosures required for compliance with the Privacy Rule.

Disclosures of PHI by Health Plan

4. From time to time relevant staff of the Health Plan will be asked to disclose PHI to other Covered Entities, regulatory agencies, law enforcement authorities and others. Many of these disclosures are permitted or required by law and do not require authorization of the individual. Others may require authorization of the individual whose PHI is to be disclosed. Except for those instances identified previously, the Health Plan will apply the minimum necessary standard to all disclosures.

Relevant staff of the Health Plan may treat a request for a disclosure as being for the minimum necessary PHI when the request is:

- A permitted disclosure to a public official who states that the disclosure is the minimum necessary;
- From another Covered Entity;
- From a professional who is a member of the Health Plan or is a Business Associate of the Health Plan if he/she states that the information is the minimum necessary needed; and
- For research purposes when the required documentation is provided.

**Requests for PHI
by Health Plan**

5. Relevant staff of the Health Plan must limit requests made by them for PHI to that which is reasonably necessary to accomplish the purpose of the request.

Entire Medical Record

6. The Health Plan will not use, disclose or request an entire medical record unless the entire medical record is specifically justified as reasonably necessary. Unjustified use, disclosure or request of an entire medical record will be considered a violation of this policy. The only exception regarding the entire medical record is when the information is provided to persons involved in the treatment of the individual.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. April 14, 2003.

References:

45 C.F.R. §§ 164.502(b), 164.514(d)

Individual's Rights to Access & Copy PHI

Policy Statement

Individuals have the right to access and copy their own protected health information (PHI) maintained/retained by the Health Plan, including any business associates on behalf of the Health Plan, in their designated record set (DRS).

Policy Interpretation and Implementation

Definition of DRS

1. A group of records maintained by the Health Plan that are:
 - a. Medical records and billing records about individuals maintained by or for the Health Plan;
 - b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Health Plan; or
 - c. Used by or for the Health Plan to make decisions about individuals.
2. The term "record" as used above means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Health Plan.

Individual's Right to Access and Copy PHI

3. An individual generally has a right to access and copy his/her PHI maintained in the DRS.

Written Request

4. Request for inspection and copying of PHI must be submitted to the HIPAA Privacy Officer in writing.

Time Frame for Retrieval of Requested PHI

5. Insofar as practical, the individual should allow at least thirty (30) days for the Health Plan to obtain requested information. Should an extension be necessary, the individual will be notified of such request. In no case may the extension exceed thirty (30) days.

Denial of Access

6. Should the individual be denied access to requested records, a written notice must be provided to the individual indicating such denial and the reason(s) for the denial.

Service Fees

7. Postage and labor charge(s) may be assessed for copying and mailing services. These charges are based on the City's Fee Schedule.

Exceptions

8. Individuals may be denied access to (1) psychotherapy notes, and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Denial of Access Without Right of Review

9. Denial of access without a right of review may occur:

- a. Where information was compiled in anticipation of litigation;
- b. Where care was provided under the direction of a correctional institution and provision of access would jeopardize health, safety, or rehabilitation; and
- c. Where information was collected in the course of research that includes treatment of the individual and the individual agreed to a *suspension* of the right of access during the research period.

Denial in Accordance with Other Applicable Law

10. Access may also be denied in accordance with other applicable law.

Denial of Access With Right of Review

11. Denial of access with a right of review may occur:

- a. Where access is determined by a licensed professional to be likely to endanger life or safety of the individual or another person; and
- b. Where access is required by the individual's representative and a licensed professional determines that such access is reasonably likely to cause substantial harm.

Individual's Right to Review by Another Licensed Professional

12. If the basis for denial of access gives the individual a *right to review*, the individual has the right to have the denial reviewed by a licensed professional who did not participate in the original denial decision. Such review will be completed within thirty (30) days of such request. The Health Plan will provide the individual with a notice of the reviewer's decision and will comply with the determination to either provide the requested information or deny access to such requested information.

Time Frame for Facility to Act Upon Individual's Request for Access

13. The Health Plan will act upon an individual's request for access to his/her DRS no later than thirty (30) days after receipt of such request, unless the time period is extended as described below:

- a. If the information to be accessed is not maintained or accessible on premises, the Health Plan will act upon such request within sixty (60) days of receipt of such request.
- b. If the Health Plan is unable to act on the request within the applicable thirty (30) or sixty (60) day period, the Health Plan may extend the time for response by thirty (30) days, provided that the individual is given a written notice of the reason(s) for the delay and the date by which a responsive action will be taken.

Denial of Access Notice

14. The Health Plan will provide a timely, written denial of access to the individual when such denials occur. Denial notices will be written in easy-to-read language and will include, as a minimum, the following information:
- a. The basis for the denial of access;
 - b. Any right of review (as applicable);
 - c. How to file a complaint with the Health Plan;
 - d. The name and telephone number of the person to whom the complaint may be filed; and
 - e. The address of the U.S. Secretary of Health and Human Services.

Access to Requested Information

15. To the extent practical, the individual will be given access to any information requested after excluding the information for which the Health Plan has grounds for denying access.

Access to Information Maintained Off Premises

16. Should the information for which access has been requested be maintained off premises or the Health Plan does not maintain/retain such information, but knows where the information is located, the Health Plan will either (a) notify the individual where to direct his/her request for access, or (b) otherwise make arrangements for the individual to access such information. This includes, but is not limited to, information maintained by a business associate on behalf of the Health Plan.

Record Retention

17. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

18. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

19. Violations of this policy will be subject to discipline.

Effective Date

20. April 14, 2004.

References:

45 C.F.R. § 164.524

Please Read Carefully and Sign

I understand that the Health Plan will provide the requested inspection or copies if required to do so under applicable law. I also understand that I may be charged for copying and postage in accordance with the Health Plan's Notice of Privacy Practices.

Signature

Date

Please note: Applicable law requires us to respond to you within 30 days after receiving your request, unless the information requested is not maintained at our primary business address, in which case we will respond within 60 days. We are entitled, in certain circumstances, to an additional 30 days in which to respond. We will send you written notice if we determine we will need the additional 30 days.

For office use only:

Received by: _____ Date: _____

GRANT OF REQUEST TO ACCESS OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Right to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request to access and/or copy your own protected health information ("PHI") on **[date]**.

ACCESS

_____ The information to which you requested access will be available as of **[date]** for your review at **City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118**.

_____ There are questions regarding your request for access. Please call us at **651-452-1850** so we may discuss the nature and scope of your request.

COPIES

_____ We have enclosed copies of the information you requested. We are permitted under federal law to recover our reasonable copying and postage costs of \$____. Please remit payment **[by check or money order]** to:

**City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118**

_____ The records you requested are voluminous or are not in a format that is easily copied and mailed. Please call us at 651-452-1850 so we may discuss the scope and format of your request, as well as a convenient time and place for you to inspect or obtain a copy of the requested information.

Please call us at 651-452-1850 if you have any questions.

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO ACCESS TO OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Rights to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request to access and/or copy your own protected health information ("PHI") on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original response due date]**.

Please call us at 651-452-1850 if you have any questions.

Thank you for your patience.

DENIAL OF REQUEST TO ACCESS OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Rights to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We have reviewed your request to access and/or copy your own protected health information ("PHI"). We are denying your request for the following reasons:

- _____ We do not maintain **[part of]** the information you requested. That information is maintained by **[insert description]**. You have no right to appeal this denial.
- _____ **[Part of the <or> The]** information you requested is not contained in our designated record sets. This means that we do not use the information you requested to make decisions relating to your health benefits. Accordingly, we are not required to provide it under the federal Privacy Rule. **[We will provide you with access to the part of the information you requested that is in our designated record sets.]** You have no right to appeal this denial.
- _____ The Privacy Rule exempts the information you requested from access requests. You have no right to appeal this denial.
- _____ We have determined that release of the information you request may result in harm to you or someone else. You may appeal this basis of denial. If you would like to appeal this determination, you may write to us at:

**City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118**

Complaints. You may submit a complaint about this denial to us. If you choose to do so, please direct your complaint as indicated below. Please note that your complaint is not considered an appeal of our denial.

**Privacy Officer
1101 Victoria Curve
Mendota Heights, MN 55118
651-452-1850**

You may also submit a complaint about this denial of access to the head of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name, and (2) a description of the acts or omissions that you believe violate our responsibilities under the Privacy Rule. Your complaint must be filed within 180 days from the date of this letter.

Please call us at 651-452-1850 if you have any questions.

Amendment of the PHI

Policy Statement

An individual may amend his/her protected health information (PHI).

Policy Interpretation and Implementation

Amendment of PHI

1. An individual may amend his/her PHI except as outlined below:
 - a. The originator of the record is no longer available;
 - b. The information the individual wishes to amend was not created by the Health Plan;
 - c. The information is not part of the health information record;
 - d. The information contained in the record is accurate and complete; and/or
 - e. The amended information would not be available as provided by current law.

Written Amendment Request

2. All requests for amendments to PHI must be submitted to the HIPAA Privacy Officer in writing.

Time Frame for Acting Upon a Request for Amendments

3. The Health Plan will act upon the individual's request for an amendment no later than sixty (60) days after receipt of such request. Should the Health Plan be unable to act upon the request within the sixty (60) day period, the individual will be provided with a written notice of the reasons for the delay and the date by which the Health Plan will complete such action. In no case will such extension extend beyond thirty (30) days.

Acceptance of Amendment

4. When the Health Plan accepts the amendment, in whole or in part, the Health Plan will:
 - a. Make the requested amendment(s) to the PHI or record that is subject to the amendment(s) or provide a link to the location of such amendment(s);
 - b. Inform the individual that the amendment(s) are accepted and have been made;
 - c. Notify persons/entities authorized by the individual that such amendments have been made and provide copies of such amendments as requested; and
 - d. Notify business associates that such amendments have been made and provide copies of such amendments to business associates as requested.

Denial of Amendment Requests

5. Should the Health Plan **deny** a requested amendment, in whole or in part, the Health Plan will:
 - a. Notify the individual in writing of the denial to make an amendment to his/her PHI. Such denial will include the following information:
 - i. The reason(s) for the denial;
 - ii. Information relative to how the individual may submit a written statement disagreeing with the denial;
 - iii. Information relative to how the individual may request that the amendment and the denial become part of the individual's permanent records; and
 - iv. Information relative to how the individual may file a complaint with the HIPAA Privacy Officer or to the U.S. Secretary of Health and Human Services.
 - b. Include on all notices to the individual the name, title, and telephone number of the contact person or office designated to receive complaints.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. April 14, 2004.

References:

45 C.F.R. § 164.526

REQUEST FOR AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of PHI

You have a right to request an amendment of your own protected health information ("PHI"). Please see the Notice of Privacy Practices **or contact the Health Plan's Privacy Officer at 651-452-1850** for more information.

Please submit this form to:
Privacy Officer, City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118

Your name: _____

Address: _____

Daytime phone number: _____

Please select one:

- I participate in or am covered under the Health Plan **[City of Mendota Heights]**.
- I am the personal representative of an individual participating in or covered under the Health Plan *(please attach completed Designation of Personal Representative form if one is not already on file)*.

I would like to request an amendment to the following information: _____

The information should be amended in the following manner: _____

I believe this information should be amended because (required): _____

Please Read Carefully and Sign

I understand that the Health Plan will agree to my requested amendment unless it may deny the request under applicable law.

Signature

Date

Please note: Applicable law requires us to respond to you within 60 days after receiving your request, unless we send you notification that we will need an additional 30 days to respond.

For office use only:

Received by: _____ Date: _____

GRANT OF AMENDMENT OF PHI REQUEST

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for amendment of your own protected health information ("PHI") on **[date]**.

We have agreed to comply with your request. Accordingly, we will **[append or link the corrected information to the PHI in our possession]**.

If you like, we will notify persons you believe have received the PHI that is the subject of your amendment request. Please fill out and return the enclosed form listing the names and, if known, addresses, of those persons or entities. Please note that you must sign the form, giving us written permission to disclose this amended information to the people you have listed.

Please call us at 651-452-1850 if you have any questions.

Enclosure

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an amendment to your own protected health information ("PHI") on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original due date of response]**.

Please call us at 651-452-1850 if you have any questions.

Thank you for your patience.

DENIAL OF REQUEST FOR AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We have reviewed your request for amendment of your own protected health information ("PHI"). Your request is denied for the following reason:

_____ We believe the records identified in your request are accurate and complete.

_____ **[Part of the <or> The]** information you requested is not contained in our designated record sets. This means that we do not use the information you requested to make decisions relating to your health benefits. Accordingly, we are not required to amend it under the federal Privacy Rule.

_____ We did not create the records identified in your request. If you believe the person or entity that created the record is no longer available to respond to a request for amendment, please notify us and we will reconsider your request.

_____ We have determined that the records you identified in your request would not be available for inspection under the "right of access" provisions of the federal Privacy Rule, and therefore are not subject to amendment.

If you disagree with our denial, you may submit a written statement setting forth the basis for your disagreement. Your statement may be no longer than 1 page. If you choose not to file a statement of disagreement, you may ask that we include your request for amendment and our denial of your request with any future disclosures of the records at issue. If you wish to pursue either option, please submit in writing (1) your statement of disagreement, or (2) your request that we include in future disclosures your amendment request and our denial of that request to:

**City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118**

You may submit a complaint about this denial to us. If you choose to do so, please direct your complaint as indicated below. Please note that your complaint is not considered an appeal of our denial.

**Privacy Officer, City of Mendota Heights
1101 Victoria Curve
Mendota Heights, MN 55118
651-452-1850**

You may also submit a complaint about this denial to the head of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name, and (2) a description of the acts or omissions that you believe violate our responsibilities under the Privacy Rule. Your complaint must be filed within 180 days of the date of this letter.

Please call us at 651-452-1850 if you have any questions.

NOTICE TO OTHERS OF AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[person or entity in possession of amended protected health information ("PHI")]**:

Please note that you may have in your records the following protected health information ("PHI") relating to **[name of participant or beneficiary]**:

[description of PHI]

We have amended that PHI as follows:

[describe amendment]

Please make a note of it in your records. This notice is being given as required by 45 CFR § 164.526, which is part of the Privacy Rule issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

[Add when notice goes to a business associate.] Under your contract with us, you are a business associate, and as such are required to append or link this notice or, if you choose, the amendment described above, to the PHI described.

Please call us at 651-452-1850 if you have any questions.

REQUESTOR'S LIST OF PERSONS OR ENTITIES TO BE NOTIFIED OF AMENDMENT

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

PERSONS OR ENTITIES TO BE NOTIFIED OF AMENDMENT

I authorize the Health Plan to notify the persons or entities listed below of the amendment the Health Plan has made to my protected health information ("PHI").

NAME OF PERSON OR ENTITY	ADDRESS

(Please attach additional pages, if needed.)

Date: _____	Signature: _____
Printed name: _____	

Please submit this form to:
Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118

Accounting of Disclosures of PHI

Policy Statement

Individuals have the right to receive an accounting of disclosures of protected health information (PHI) made by the Health Plan, including any business associate on behalf of the Health Plan.

Policy Interpretation and Implementation

Request for an Accounting of Disclosures of PHI

1. An individual or his/her representative may request an accounting of disclosures of his/her PHI made by the Health Plan, including any business associate on behalf of the Health Plan, during a specified time period of up to six (6) years prior to the date of the request of an accounting. Disclosures must be tracked by the Health Plan for purposes of an accounting except the following disclosures:
 - a. To carry out treatment, payment or healthcare operations (TPO) as permitted under current law;
 - b. To the individual about his/her own PHI;
 - c. To persons involved in the individual's care;
 - d. For national security purposes;
 - e. Pursuant to the individual's authorization;
 - f. To federal/health department officials as permitted under current law; and
 - g. Those disclosures that occurred *prior* to April 14, 2004.

Time Frame of Accounting Reports

2. Other than the exceptions noted above, the accounting record must include disclosures of PHI that occurred during the six (6) years (or shorter time period as is specified in the request) prior to the date of such request, including disclosures made by or to any of the Health Plan's business associates.

Content of Accounting of Disclosures Record

3. The content of the written accounting of disclosures record must contain, at a minimum, the following information:
 - a. Date of the disclosure;
 - b. Name of the entity or individual who received the PHI
 - c. The address of the person receiving the PHI (if known)
 - d. A brief description of the PHI disclosed; and

- e. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu thereof, a copy of the individual's authorization or the request for the disclosure.

Multiple Disclosures

- 4. If, during the time period for the accounting, *multiple* disclosures have been made to the same entity or individual for a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth in paragraph 3 above for the first disclosure, and then summarize the frequency of number of disclosures made during the accounting period and the date of the last disclosure during the accounting period.

Time Frame for Providing Accounting of Disclosure Data

- 5. An individual's request for an accounting of PHI disclosures must be provided to the individual or representative within sixty (60) days of such request. If unable to provide the accounting within the sixty (60) day time frame, a one time thirty (30) day extension may be provided if:
 - a. The individual is notified in writing of the delay;
 - b. The notice includes the reason(s) why the delay is necessary; and
 - c. The notice includes the date by which the accounting will be provided.

Log

- 6. The Health Plan will keep a log of all disclosures required by paragraph 1 above which will include all necessary information.

Record Retention

- 7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

- 8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

- 9. Violations of this policy will be subject to discipline.

Effective Date

- 10. April 14, 2004.

References:

45 C.F.R. § 164.528

REQUEST FOR AN ACCOUNTING OF DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

You have a right to request that the Health Plan provide you with an accounting of certain disclosures that it has made of your protected health information ("PHI"). Please see the Health Plan's Notice of Privacy Practices **or contact the Health Plan's Privacy Officer at 651-452-1850** for information.

Please submit this form to: **Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118**

Your name: _____

Address: _____

Daytime phone number: _____

Please select one:

- I participate in or am covered under the Health Plan **[City of Mendota Heights]**.
- I am the personal representative of an individual participating in or covered under the Health Plan **[City of Mendota Heights]** (*please attach proof of personal representative status*).

I would like an accounting of covered disclosures of my PHI made by the Health Plan between the following dates:

_____ and _____.

Note: We are not required to provide an accounting of disclosures we made prior to the effective date of the federal privacy rules (April 14, 2004).

Please Read Carefully and Sign

I understand that the Health Plan will provide the requested accounting of disclosures if required to do so under applicable law. If this is not my first request for an accounting within a 12-month period, I understand that the Health Plan will notify me of its reasonable costs for complying with my request and provide me with the opportunity to agree to pay those charges in order to receive the requested accounting.

Signature

Date

Please note: Applicable law requires us to respond to you within 60 days after receiving your request, unless we send you a notification that we will need an additional 30 days to respond.

For office use only:

Received by: _____ Date: _____

ACCOUNTING OF DISCLOSURES OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information ("PHI") on **[date]**. We set forth below an accounting of those disclosures that, by law, must be provided in response to your request.

Information Disclosed	Date Disclosed	Disclosed To:	Purpose of Disclosure
	[Note: For multiple disclosures to the same entity, include all information for first such disclosure, how often or when subsequent disclosures were made, and the date of the last disclosure.]	[Note: Include contact information, if known.]	[Note: If disclosure was made pursuant to a written request, you may include copies of the written request instead of describing the purpose of the disclosure.]

There is no charge for this accounting. However, if you request additional accountings within the next 12 months, there may be a charge to you for our costs in complying with your requests.

Please call us at 651-452-1850 if you have any questions.

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO ACCOUNTING REQUEST

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information ("PHI") on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original due date of response]**.

Please call us at 651-452-1850 if you have any questions.

Thank you for your patience.

NOTIFICATION OF CHARGES FOR SECOND REQUEST IN 12 MONTH PERIOD

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information ("PHI") on **[date]**. We responded to a prior request from you for an accounting on **[date]**. You are entitled to one accounting without charge during any 12 month period. Because this is your second request within 12 months, we will charge you **[\$___]** for our reasonable costs in putting together the accounting. These costs include the time and expense of reviewing our records.

If we do not hear from you within **[30] days** from the date of this letter, we will assume that you have withdrawn your request. If you do not wish to withdraw your request, please sign the acknowledgement at the bottom of this letter and return it within **[30] days**.

Please call us at 651-452-1850 if you have any questions.

Thank you for your patience.

ACKNOWLEDGMENT

I, _____, understand that I am being charged \$___ for my most recent request for an accounting of disclosures of my protected health information ("PHI") because I have requested more than one accounting within a 12 month period. I agree to pay all reasonable charges prior to receiving the accounting. A check or money order is enclosed.

Name (print)	Signature
Telephone Number	Date

Return acknowledgement to:
Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118

Verification Prior to Disclosure of PHI

Policy Statement

Prior to disclosing PHI, the Health Plan must verify the identity of the recipient and the recipient's authority to have access to PHI, unless the identity and authority are known to the Health Plan. In addition, when it is a condition of disclosure, prior to the disclosure of PHI, the Health Plan must obtain any documentation, statements, or representations of the recipient as required by the Privacy Rule.

Please note: This Policy relates to Form 4, Use and Disclosure of PHI, Form 6, Individual's Right to Access & Copy PHI, and Form 19, Disclosures to the Plan Sponsor.

Policy Interpretation and Implementation

Responsibility For Obtaining Verifications

1. The HIPAA Privacy Officer or his/her designee will be responsible for obtaining verifications when disclosure of PHI is necessary.

Verification of Identity and Authority

2. Before releasing PHI, sufficient information must be obtained from the person requesting the information to reasonably conclude, under the circumstances, that the person is who he/she says he/she is and has authority to have access to the PHI. The type of information required will depend on the nature of the request, from whom it is made, and the method in which it is made.

Request for Information In Person

3. When a request for PHI is made in person, identity may generally be verified by inspecting some form of photo identification. If photo identification is unavailable, identity may be verified by inspection of some other form of government issued identification.

In addition, in cases of disclosure for public policy purposes, authority to have access to PHI may generally be verified by receipt of the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) of the subject of the PHI and:

- a. A written statement of the authority under which the PHI is requested (or if a written statement is impracticable, an oral statement); or
- b. A legal document, such as a warrant, subpoena, court order, or other legal process.

Request for Information By Telephone

4. When a request for PHI is made by telephone, identity may generally be verified by receipt of information that identifies the person requesting the information. For instance, if the person requesting the PHI is the subject of the PHI, then identity may be established by providing his/her full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number). When the

person requesting the information is a third party (i.e. health care provider), identity may be established by obtaining the caller's telephone number and calling

him/her back, making sure the area code and exchange matches a listed telephone number for the company/agency. In order to verify authority to access the PHI when it is requested by someone other than the subject, obtain the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) regarding the subject of the PHI and a statement of the authority under which the PHI is requested.

Please note: The Health Plan is not required to release PHI when the request for release is made by telephone.

Request for Information By Mail or Email

5. If a request for PHI is received by mail, identity may generally be verified by receipt of some unique piece of information that identifies the person requesting the information or by receipt of the request in a format that tends to establish the identity of person making the request. For instance, if the person requesting the PHI is the subject of the PHI, then a written request containing the person's social security number or other unique identification number will be sufficient. When the person requesting the information is a health care provider or a public agency, receipt of the request on appropriate letterhead will be sufficient.

Verification of Documentation, Statements, or Representations

6. The person verifying the documentation, statements, or representations provided by the recipient as required by the Privacy Rule may, when doing so is reasonable under the circumstances, rely on documentation, statements, and representations that, on their face, meet the applicable requirements. Such reliance will not be reasonable when information is known by the person that tends to indicate the documentation, statement, or representation is not authentic. In such situations, additional steps to verify the authenticity of the documentation, statement, or representation shall be taken.

Log

7. The Health Plan will keep a log of all verifications, which will include all necessary information.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the

contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. April 14, 2004.

References:

45 C.F.R. § 164.508(b)

Individual Requested Restrictions on Use or Disclosure of PHI

Policy Statement

Individuals have the right to request restrictions on uses and disclosures of protected health information (PHI) relative to treatment, payment, or health care operations (TPO).

Policy Interpretation and Implementation

Request for Restriction on use or Disclosure of PHI

1. A request for restriction of use or disclosure of information must be submitted in writing to the HIPAA Privacy Officer. Such request must specify the type of information to be included in the restriction and to whom the restriction applies.
2. Upon receipt of an individual's request that a restriction be placed on the use or disclosure of PHI, the HIPAA Privacy Officer will:
 - a. Determine the reasonableness of the request based on the administrative capability of the Health Plan to comply with such request;
 - b. Identify the means and location the individual wishes the information to be communicated; and
 - c. Notify the individual whether or not the Health Plan agrees to the restriction within sixty (60) days of the date of such request unless an extension is necessary. Such extension will not exceed thirty (30) days.

Exceptions to Restrictions

3. Should the Health Plan agree to the restriction, the Health Plan and its business associates will honor such request except when:
 - a. The restriction is terminated by the Health Plan or the individual, and/or
 - b. There is an emergency treatment situation.

The HIPAA Privacy Officer will be responsible for notifying any impacted business associates.

Emergency Treatment

4. When emergency treatment is necessary, the provider of the treatment may not use or disclose PHI or information which a restriction has been placed, except for what is necessary to provide appropriate emergency care for the individual. The emergency health treatment provider may not further disclose the restricted information beyond what is needed for the emergency treatment.

Termination of a Restriction

5. The Health Plan may terminate a restriction:

- a. When the individual requests the termination;
and/or
- b. When the Health Plan informs the individual of
the termination.

Termination Notices

6. Termination notices must be in writing and must indicate the effective date such termination and the reason(s) for such termination.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. April 14, 2004.

References:

45 C.F.R. § 164.522

REQUEST TO RESTRICT CERTAIN USES AND DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Form 10, Individual Requested Restrictions on Use or Disclosure of PHI.

You have a right to request the Health Plan restrict:

- Uses or disclosures of your protected health information ("PHI") in carrying out payment or health care operations activities.
- Disclosures to family members or friends involved in your health care or payment relating to your health care.

Use this form to request such a restriction. **THE HEALTH PLAN IS NOT REQUIRED TO COMPLY WITH YOUR RESTRICTION REQUEST.**

IMPORTANT: IF YOU BELIEVE YOU WILL BE ENDANGERED IF YOUR PHI IS DISCLOSED THROUGH A COMMUNICATION WE MIGHT MAKE TO YOU OR SOMEONE IN YOUR HOUSEHOLD, PLEASE SUBMIT THE FORM ENTITLED "REQUEST FOR CONFIDENTIAL COMMUNICATION."

Please submit this form to:

Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118

Your name: _____

Address: _____

Daytime phone number: _____

Please select one:

___ I participate in or am covered under the Health Plan [**City of Mendota Heights**].

___ I am the personal representative of an individual participating in or covered under the Health Plan (*please attach completed Designation of Personal Representative form*).

___ I request the Health Plan to restrict its uses or disclosures of my PHI for purposes of payment or health care operations. Specifically, I request the following restrictions (describe):

(If more space needed, please attach separate sheet)

_____ I request the Health Plan to not make disclosures to the following family members or friends who may be involved in my health care or payment with respect to my health care (list names):

(If more space needed, please attach separate sheet)

Please Read Carefully and Sign

I understand that the Health Plan is not required to agree to my requested restriction. I also understand that if the Health Plan agrees to the requested restriction, it may stop doing so prospectively so long as it informs me that the restriction is removed.

Signature

Date

For office use only:

Received by: _____ Date: _____

RESPONSE TO REQUEST TO RESTRICT CERTAIN USES AND DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Policy Form 10, Individual Requested Restrictions on Use or Disclosure of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request that we restrict certain uses and disclosures of your protected health information ("PHI"). As you know, the law does not require us to agree to your requested restriction.

_____ We **will not** be able to agree to your restriction. However, if you believe you will be endangered if your PHI is disclosed through a communication we might make to you or someone in your household, please submit the form entitled "Request For Confidential Communication."

_____ We **will** agree to restrict uses and disclosures of your PHI as you requested. Specifically, **[describe uses and disclosures that will not be made, including specifically the names of family members/friends to whom disclosures will not be made.]**

Please note that we may remove this restriction prospectively at any time upon providing notice to you.

Please call us at 651-452-1850 if you have any questions.

Individual Requested Restrictions on Confidential Communications

Policy Statement

Individuals have the right to request an alternate means of communication of the individual's protected health information (PHI) from the Health Plan to the individual. The restrictions apply only to communications to the individual by the Health Plan or communications that would otherwise go to the subscriber of the policy under which the individual has coverage. The effect of this is to ensure a family member who is not the subscriber can receive communications of PHI at the individual's workplace or other alternate address or phone number, so that other family members are unaware of the information.

Policy Interpretation and Implementation

Request for Confidential Communications

1. A request for confidential communications must be submitted in writing to the HIPAA Privacy Officer. Such request must specify the type of information to be covered by the confidential communication's restriction, and to whom the restriction applies, the alternate address or other method of contact requested, and how payment will be handled (if applicable). The Health Plan may require evidence that if the information is disclosed other than the manner requested it could endanger the individual.

Consideration of Request

2. Upon receipt of an individual's written request for confidential communications of PHI, the HIPAA Privacy Officer will:
 - a. Determine the reasonableness of the request based on the administrative capability of the Health Plan to comply with such request;
 - b. The determination of reasonableness will not include an evaluation of the merits of the individual's reason for making the request;
 - c. Identify the alternate means by and/or location to which the individual requests the information to be communicated and how payment will be handled; and
 - d. Notify the individual whether or not the Health Plan agrees to the request within sixty (60) days of the date such request was received unless an extension is necessary. Such extension shall not exceed thirty (30) days.

Exceptions to confidential communications

3. Should the Health Plan agree to the confidential communications, the Health Plan and its business associates will honor such request except when the confidential communication request is terminated by the Health Plan or the individual. The HIPAA Privacy Officer will be responsible for notifying any impacted business associates.

Termination of confidential communications

4. The Health Plan may terminate confidential communications:
 - a. When the individual requests the termination; and/or
 - b. When the Health Plan informs the individual of the termination.

Termination Notices

5. Termination notices must be in writing and must indicate the date such termination is to become effective and the reason(s) for such termination. The termination notice must be provided before the effective date of the termination notice. A copy of the termination notice must be filed in the individual's records maintained for HIPAA purposes.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. April 14, 2004.

References:

45 C.F.R. § 164.522(b)

REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Please note: This Administrative Form relates to the Health Plan's Policy Form 11, Individual Requested Restrictions on Confidential Communications.

You have a right to request that the Health Plan provide alternative means or alternative locations for you to receive communications of your protected health information ("PHI"). We must agree to your request for a confidential communication **only** if (1) you provide a reasonable alternative means or locations for the communication, and (2) you believe that a disclosure of the information could endanger you.

Please submit this form to:

Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118

Your Name: _____

Address: _____

Daytime phone number: _____

Please select one:

- I participate in or am covered under the Health Plan **[City of Mendota Heights]**.
- I am the personal representative of an individual participating in or covered under the Health Plan **[City of Mendota Heights]** (*please attach completed Designation of Personal Representative form*).

My request for confidential communications from the Health Plan applies to the following types of communications (list):

(If more space is needed, please attach a separate sheet)

The communications identified above should be made to me in the following manner (please provide an alternative address, telephone number, or e-mail address):

Please Read Carefully and Sign

I believe that disclosure of my PHI in the communications described above could endanger me. I understand that the Health Plan is not required to agree to my request for a confidential communication if I do not provide a reasonable alternative means for the communications or if I do not believe that the disclosure of information in the communication will endanger me.

Signature

Date

For office use only:

Received by: _____ Date: _____

Privacy Complaint Procedure

Policy Statement

Individuals, family members, employees, the general public, or business associates have the right to file complaints regarding Health Plan policies, procedures, or practices relative to the access, use, or disclosure of protected health information (PHI).

Policy Interpretation and Implementation

Designation of Person to Receive Complaints

1. The HIPAA Privacy Officer has been designated as the individual responsible for receiving, processing, and investigating all privacy related complaints. The HIPAA Privacy Officer may in turn designate employees in particular areas to assist.

Filing of Privacy Complaints

2. Any individual, representative, family member, employee, business associate, visitor, or the general public may file a grievance or complaint regarding Health Plan privacy practices (e.g., denial of access to PHI, amendment of health records, problems with business associates, HIPAA policy and procedure violations, etc.) without fear or reprisal or retaliation in any form.

Submitted Complaints

3. Complaints should be submitted to the HIPAA Privacy Officer in writing.

Investigation Process

4. The HIPAA Privacy Officer or his/her designee will begin an investigation into allegations within five (5) working days of the receipt of the complaint.

Results of Investigation

5. A written report of the findings of the investigation will be provided to the individual filing the complaint within thirty (30) days of receiving such complaint unless an extension is necessary to complete the investigation. Such extension may not exceed thirty (30) days.

Dissatisfaction of Investigation/Resolution

6. Should the individual not be satisfied with the result of the investigation, or the recommended resolution(s), he/she may file a complaint with the Secretary of Health and Human Services (HHS).

Filing Complaints with the Secretary of HHS

7. Complaints may be filed directly with the Secretary of HHS. Such complaints must be in writing, identify the Health Plan, and must describe the violation. Complaints must be filed within one-hundred eighty (180) days of the complainant learning of the alleged violation or should have been aware of the alleged violation.

Address of Secretary of HHS

8. The address of the Secretary of HHS is located in the Notice of Privacy Practices (NPP) and/or made available to individuals. Persons may also obtain the address from the HIPAA Privacy Officer.

Retention of Complaints Log

9. The HIPAA Privacy Officer or his/her designee will maintain a log of all complaints received. Copies of all complaints, their disposition and resolutions, and our complaint log will be maintained for a period of at least six (6) years from the date such complaint was received.

Record Retention

10. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

11. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

12. Violations of this policy will be subject to discipline.

Effective Date

13. April 14, 2004.

References:

45 C.F.R. § 164.530(d)

PRIVACY COMPLAINT FORM

Please note: This Administrative Form relates to the Health Plan's Policy Form 12, Privacy Complaint Procedure.

You have a right to file a complaint about the Health Plan's privacy practices or the Health Plan's compliance with the Notice of Privacy Practices, Privacy Policies and Procedures, or the federal Privacy Rule. The Health Plan will not require you to waive any right you may have under the federal Privacy Rule to file your complaint, nor will filing your complaint adversely affect your enrollment in the Health Plan, your eligibility for benefits under the Health Plan, or payment of your claims under the Health Plan.

Please submit this form to:

Privacy Officer, City of Mendota Heights, 1101 Victoria Curve, Mendota Heights, MN 55118

Your name: _____

Address: _____

Daytime phone number: _____

Please provide a concise statement of your complaint:

Date: _____ Signature: _____

Printed name: _____

For office use only:

Received by: _____ Date: _____

RESPONSE TO PRIVACY COMPLAINT

Please note: This Administrative Form relates to the Health Plan's Policy Form 12, Privacy Complaint Procedure.

Dear **[participant, beneficiary, or personal representative]**:

We received your complaint regarding the Health Plan's handling of your protected health information ("PHI"). The privacy of PHI is important to us and we take it seriously. You stated that **[brief description]**.

___ [We have investigated this matter and determined that no violation of our privacy policies and procedures or the Privacy Rule occurred.] **[Brief description of why use/disclosure was proper or policies/procedures are appropriate.]**

___ [We have investigated this matter and determined that a violation of **[brief description]** has occurred.] **[Brief description of what is being or has been done.]**

Please call us at 651-452-1850 if you have any questions.

COMPLAINT TRACKING LOG

Please note: This Administrative Form relates to the Health Plan’s Policy Form 12, Privacy Complaint Procedure.

Name of Individual Logging Complaint	Date Rec’d	Nature of Complaint	Covered Component ³	Start Date of Investigation	Investigation Completion Date	Date Response Issued to Individual Logging Complaint	Action Taken

³ For covered entities who are a part of an Organized Health Care Arrangement (OHCA), record which covered component is affected by the complaint.

Authorization for Use or Disclosure of PHI

Policy Statement

All uses and disclosures of protected health information (PHI) beyond those otherwise permitted by current HIPAA law, and not otherwise prohibited under another applicable law, require a signed authorization. In addition, the Health Plan, including any business associates on behalf of the Health Plan, may choose to obtain a signed authorization in situations where it is not required.

Policy Interpretation and Implementation

Responsibility For Obtaining Authorizations

1. The HIPAA Privacy Officer or his/her designee will be responsible for obtaining authorizations when use or disclosure of protected health information is necessary.

Provision of Treatment, Payment, or Eligibility

2. The provision of treatment, payment, or eligibility for benefits may not be conditioned on the individual's provision of an authorization for the use or disclosure of PHI.

Content of Authorization

3. Each authorization for the use or disclosure of an individual's PHI will be written in easy to read language and will include, at a minimum, the following information:
 - a. A specific and meaningful description of the information to be used or disclosed;
 - b. The name or identification of the person or class of person(s) authorized to make the use or disclosure;
 - c. The name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;
 - d. An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure; the authorization shall state that it will expire after ninety (90) days unless the individual has opted for a shorter or longer time. An individual may specify a longer period of time for the duration of the authorization only if the person:
 - i. Is part of an approved research study and has given authorization for a longer period of time; or
 - ii. Is expected to continue receiving services beyond ninety (90) days and has given authorization for a longer period of time, which may be up to one calendar year.
 - e. A statement of the individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how

the individual may revoke the authorization. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the facility, program or individual has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law; (See policy entitled *Revocation of an Authorization.*)

- f. A statement that the information may only be re-released with the written authorization of the individual, except as required by law;
- g. The dated signature of the individual; and
- h. If the authorization is signed by a personal representation of the individual, a description of the representative's authority to act on behalf of the individual.

Request Form

- 4. The Health Plan may develop a standard form for authorizing use and disclosure of PHI. If the Health Plan develops a form, the form must be used for all authorizations.

Requests to Use or Disclose PHI for Own Purposes

- 5. If the authorization is requested by the Health Plan for its own use or disclosure of the PHI it maintains, for purposes outside of treatment, payment or health care operations (TPO), health care oversight or public health activities, the following elements are required in addition to those specified in paragraph 3 above:
 - a. Except in circumstances where it is allowed, a statement that treatment, payment and eligibility for benefits will not be conditioned upon the individual's provision of an authorization;
 - b. A description of each purpose of the requested use or disclosure;
 - c. A statement that the individual may refuse to sign the authorization;
 - d. If applicable, a statement that the use or disclosure will result in direct or indirect remuneration for a third party; and
 - e. A copy of the signed authorization provided to the individual.

Requests for PHI from Others

- 6. If the authorization is requested for disclosures of PHI by others, the following elements are required in addition to those specified in paragraph 5 above:
 - a. A description of each purpose of the requested disclosure;
 - b. Except in circumstances where it is allowed, a

statement that treatment, payment and eligibility for benefits will not be conditioned upon the individual's provision of an authorization;

- c. A statement that the individual may refuse to sign the authorization; and
- d. A copy of the signed authorization provided to the individual.

Use or Disclosure of PHI for Research

- 7. Use or disclosure of PHI created for research generally requires an authorization unless such use or disclosure is permitted by law. Such authorization must include the basic elements specified in paragraphs 3, 5, and 6 above, as well as the following information:
 - a. A description of the extent to which PHI will be used to carry out TPO;
 - b. A description of any PHI that will not be used or disclosed for purposes otherwise permitted, provided that the limitation may not preclude disclosures required by law or to avert serious threat to health or safety; and
 - c. References to any privacy notice expected to be given to the individual, which must include statements that the terms outlined in the privacy notice are binding.
- 8. The authorization for the use and disclosure of PHI created for research may be combined in the same document with the consent to participate in research, or the privacy notice.

Record Retention

- 9. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

- 10. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

- 11. Violations of this policy will be subject to discipline.

Effective Date

- 12. April 14, 2004.

References:

45 C.F.R. § 164.508(b)

AUTHORIZATION FOR USE OR DISCLOSURE

Please note: This Administrative Form relates to the Health Plan's Policy Form 13, Authorization for Use or Disclosure of PHI.

Name: _____ Date: _____

I hereby authorize the use and disclosure of my protected health information ("PHI") as indicated below. I understand that this authorization is voluntary and that I may revoke this authorization at any time except to the extent that action has been taken in reliance on this authorization. I also understand that if the individual or organization authorized to receive this information is not required to comply with current Privacy Rule, my PHI may be disclosed to others and no longer protected by the current federal Privacy Rule.

- | | |
|---|--|
| <input type="checkbox"/> Complete health care record(s) | <input type="checkbox"/> Progress Notes |
| <input type="checkbox"/> History & Physical Examination | <input type="checkbox"/> Care Plans |
| <input type="checkbox"/> Laboratory Reports | <input type="checkbox"/> Dental Records |
| <input type="checkbox"/> Medical/Treatment Records | <input type="checkbox"/> Photographs, Video Tapes, Digital or other images |
| <input type="checkbox"/> Pathology Reports | <input type="checkbox"/> Billing Statements |
| <input type="checkbox"/> X-Ray Reports | <input type="checkbox"/> Emergency Care Records |
| <input type="checkbox"/> Transcribed Reports | <input type="checkbox"/> Consultant Reports |
| <input type="checkbox"/> Nurses' Notes | <input type="checkbox"/> Discharge Summary |
| <input type="checkbox"/> Other: _____ | |

The information checked and/or listed above is to be released to: _____,
for the purposes of:

- Assisting with claims resolution
- Insurance or other benefit eligibility or coverage
- Litigation, potential litigation, or other adversarial proceedings
- Fitness for duty determination, drug testing results, or other employment-related purposes
- Other: _____

This authorization, for the release of the PHI checked and/or listed above, is valid for one (1) year after the date it is signed or upon completion of the use of the information for the purpose it was intended, unless an earlier expiration date is indicated here: _____.

I understand that the individual, organization, or entity receiving my PHI may receive financial or in-kind compensation in exchange for using or disclosing the PHI described above.

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits.

I understand that I may access and copy any PHI used or disclosed under this authorization. I understand that a fee may be charged for such copying services.

I hereby release the Health Plan, its employees, officers, and health care professionals from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

I understand that I may revoke this request at anytime by providing the Health Plan with my written notice of such revocation.

Date: _____	Signature: _____
	Printed name: _____
	<i>or</i>
Date: _____	Signature of personal representative: _____
	Printed name of personal representative: _____
	Relationship to me and basis upon which can sign: _____

Date: _____	Signature of witness: _____
	Printed name of witness: _____

Revocation of an Authorization

Policy Statement

Individuals have the right to revoke the authorization to access, release, use or disclose their protected health information (PHI) at any time. (Also see policy entitled: *Authorization for Use or Disclosure of PHI.*)

Policy Interpretation and Implementation

Revocation Request

1. All requests for revocation of an individual's authorization to access, release, use, or disclose PHI must be submitted to the HIPAA Privacy Officer in writing. The revocation must be specific enough to permit identification of the authorization that is being revoked. Oral requests will not be honored.

Notification of Personnel of a Revocation

2. Upon receipt of a written revocation, the HIPAA Privacy Officer will notify relevant staff and impacted business associates that a revocation has been received and that no further information may be released as specified in the authorization, with the exception that personnel may, as a result of relying on the authorization:

Exceptions to Revocation

- a. Complete the task it started (e.g., billings for services already provided); or,
- b. Submit findings from an independent medical examiner to the person/entity requesting it.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

5. Violations of this policy will be subject to discipline.

Effective Date

6. April 14, 2004.

References:

45 C.F.R. § 164.508(b)(5)

REVOCACTION BY SUBJECT OF PROTECTED HEALTH INFORMATION

Please note: This Administrative Form relates to the Health Plan's Policy Form 10 (Individual Requested Restrictions on Use or Disclosure of PHI), Policy Form 11 (Individual Requested Restrictions on Confidential Communications), Policy Form 13 (Authorization for Use or Disclosure of PHI), Policy Form 14 (Revocation of an Authorization), and Policy Form 18 (Personal Representative).

Name: _____ Date: _____

I hereby revoke the following authorization and/or restriction, effective immediately:

- Authorization for Use or Disclosure
- Designation of Personal Representative
- Requested Restriction on Use or Disclosure
- Request for Confidential Communications
- Other: _____
- Other: _____
- Other: _____

I understand that I cannot revoke any action already taken by the Health Plan in reliance upon my authorization and/or restriction prior to the date of this revocation.

I understand that this revocation removes all authorizations and/or restrictions previously in place, and if I want to impose future authorizations or restrictions regarding my PHI, I will have to submit a new completed form to the Health Plan.

Date: _____	Signature: _____
	Printed name: _____
	<i>or</i>
Date: _____	Signature of personal representative: _____
	Printed name of personal representative: _____
	Relationship to me and basis upon which can sign: _____

Date: _____	Signature of witness: _____
	Printed name of witness: _____

For office use only:

Received by: _____ Date: _____

Business Associates & Business Associate Agreements

Policy Statement

The Health Plan may disclose protected health information (PHI) to business associates, or allow business associates to create or receive PHI, provided the business associate executives sign a written agreement to appropriately safeguard such PHI.

Policy Interpretation and Implementation

- | | |
|---|---|
| Definition of Business Associate | 1. A business associate, means a person or entity who is not an employee or workforce member of the Health Plan, who performs or assists in the performance of a function or activity on behalf of the Health Plan that involves the use or disclosure of PHI, or provides legal, actuarial, accounting, consulting, data compilation, management, administrative, accreditation, or financial services. |
| Definition of Employee/Workforce Member | 2. An employee/workforce member, for the purposes of this policy, means any employee, trainee, volunteer, , or any other person(s) whose conduct, in the performance of work for the Health Plan, is under the direct control/supervision of the Health Plan, regardless of payment source. |
| Identification of Business Associates | 3. It is the Health Plan's obligation to ensure that all of the Health Plan's business associates have a written valid business associate agreement. |
| Content of Business Associate Agreements | 4. The business associate agreement between the Health Plan and the business associate establishes permitted and required uses or disclosure of PHI. Pursuant to the agreement the business associate must agree to at least: <ul style="list-style-type: none">a. Not use or disclosure PHI;b. Develop safeguards to prevent unauthorized use or disclosure of information;c. Promptly report unauthorized access, use or disclosure of information to the HIPAA Privacy Officer;d. Require any subcontractors to adhere to the same requirements as outlined in the agreement between the Health Plan and business associate;e. Make information available for access by the individual or his/her representative as permitted by law;f. Allow individuals to amend medical information and incorporate such |

amendments as part of the PHI;

- g. Develop a process that allows for an accounting of uses and disclosures of information in accordance with current law;
- h. Make its internal practices, books and records relating to its receipt or creation of PHI available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the Health Plan's compliance with HIPAA regulations;
- i. Develop a process for returning or destroying all PHI upon termination of the business associate agreement; and
- j. Develop a process for continuing the full protection of PHI for as long as the business associate retains any PHI.

Record Retention

- 5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

- 6. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about your HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

- 7. Violations of this policy will be subject to discipline.

Effective Date

- 8. April 14, 2004.

References:

45 C.F.R. § 164.504(e)

HIPAA ADMINISTRATIVE SIMPLIFICATION AGREEMENT

This Agreement is entered into by and between the City of Mendota Heights on behalf of **City of Mendota Heights** ("Covered Entity") and **<<name of business associate>>** ("Business Associate").

SECTION 1 – DEFINITIONS

1.1 **Definitions.** The following definitions are used by this Agreement:

- a) Business Associate – means **<<name of business associate>>**.
- b) Covered Electronic Transactions – shall have the meaning given to the term "transaction" in 45 C.F.R. Section 160.103.
- c) Covered Entity – means **City of Mendota Heights**.
- d) Covered Individual – means a person who is eligible for payment of certain services or supplies rendered or sold to the person or the person's eligible dependents under the terms, conditions, limitations, and exclusions of a health benefit program of the Plan.
- e) Data – means formalized representation of specific facts or concepts suitable for communication, interpretation, or processing by people or automatic means.
- f) Data Aggregation – means, with respect to Protected Health Information created or received by Business Associate in its capacity as a business associate (as that term is defined in 45 C.F.R. Section 160.103) of the Plan, the combining of such Protected Health Information by Business Associate with the Protected Health Information received by Business Associate in its capacity as a business associate of another covered entity (as those terms are defined in 45 C.F.R. Section 160.103), to permit data analyses that relate to the health care operations of the respective covered entities.
- g) Data Transmission – means automated transfer or exchange of Data, pursuant to the terms and conditions of this Agreement, between the Plan and Business Associate by means of their respective Operating Systems.
- h) Designated Record Set – means a group of records maintained by or for the Covered Entity that is (1) the medical records and billing records about Individuals maintained by or for the Covered Entity, (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Covered Entity, or (3) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. As used herein, the term "Record" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for the Covered Entity.
- i) Electronic Data Interchange (EDI) – means the automated exchange of business documents from application to application.

- j) Envelope – means the control structure in a format mutually agreeable to the Plan and Business Associate for the electronic interchange of one or more encoded Data Transmissions between the Plan and Business Associate.
- k) HHS – means the United States Department of Health and Human Services.
- l) Individual – shall have the same meaning as the term “individual” in 45 C.F.R. 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. 164.502(g).
- m) Operating System – means the equipment, software, and trained personnel necessary for a successful Data Transmission.
- n) Plan – means **City of Mendota Heights**.
- o) Privacy Rule – means the Standards and Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
- p) Protected Health Information – shall have the same meaning as the term “protected health information” in 45 C.F.R. 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- q) Provider – means a hospital or professional practitioner duly certified or licensed to provide health care services to Covered Individuals.
- r) Required By Law – shall have the same meaning as the term “required by law” in 45 C.F.R. 164.501.
- s) Secretary – means the Secretary of the Department of Health and Human Services or his/her designee.
- t) Security Access Codes – means alphanumeric codes that the Plan assigns to Business Partner to allow Business Partner access to the Plan’s Operating System for the purpose of executing Data Transmissions or otherwise carrying out this Agreement.
- u) Security Incident – shall have the same meaning as the term “security incident” in 45 C.F.R. Section 164.304.
- v) Security Rule – means the Security Standards and Implementation Specifications at 45 C.F.R. Part 160 and Part 164, subpart C.
- w) Source Documents – means documents containing Data that are or may be required as part of a Data Transmission concerning a claim for payment of charges for medical services that a Provider furnishes.
- x) Standards for Electronic Transactions Rule - means the final regulations issued by HHS concerning standard transactions and code sets under the Administrative Simplification provisions of HIPAA, 45 C.F.R. Part 160 and Part 162.
- y) Trade Data Log – means the complete, written summary of Data and Data Transmissions exchanged between the Covered Entity and Business Associate over the period of time this Agreement is in effect and includes, without limitation, sender and receiver information, transmission date and time, and general nature.

SECTION 2 – BUSINESS ASSOCIATE PROVISIONS

- 2.1 **Introduction.** Business Associate, on behalf of Covered Entity, performs or assists in the performance of functions and activities that may involve the use and disclosure of Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Parts 160 and 164 (“Privacy Regulations”). This Section 2 is intended to meet the requirements of the “business associate” provisions of Privacy Rule and will govern the terms and conditions under which the Business Associate may use or disclose Protected Health Information.
- 2.2 **Permitted Uses and Disclosures.**
- a) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity pursuant to any services agreement with the Business Associate and as permitted or required by this Agreement or the Privacy Rule.
 - b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of its business or to carry out its legal responsibilities.
 - c) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of its business, if
 - i. the disclosures are required by law, or
 - ii. Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will be held confidentially and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to such person, and the person will notify the Business Associate of any instances of which the person is aware in which the confidentiality of the information has been breached.
 - d) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. Section 164.504(e)(2)(i)(B).
 - e) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. Section 164.502(j)(1).
- 2.3 **Limitations on Uses and Disclosures.** With respect to Protected Health Information that Business Associate creates or receives on behalf of Covered Entity, Business Associate will not use or further disclose the Protected Health Information other than as permitted or required by this Agreement or as Required by Law.
- 2.4 **Additional Obligations of Business Associate.** Except as otherwise specified herein, the provisions of this Paragraph 2.4 apply only to Protected Health Information that Business Associate creates or receives on behalf of Covered Entity.
- a) Safeguards. Business Associate will use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement.

- b) Reporting and Mitigation. Business Associate will report to Covered Entity any use or disclosure of Protected Health Information by Business Associate not provided for by this Agreement within ten (10) business days of its discovery by Business Associate. Business Associate agrees to promptly mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure in violation of this Agreement.
- c) Agents and Subcontractors. Business Associate will ensure that any agent or subcontractor to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply by and through this Agreement to Business Associate with respect to such information.
- d) Access to Designated Record Set. Within fifteen (15) days of a request by the Covered Entity for access to Protected Health Information about an Individual, Business Associate shall make available to the Covered Entity or, as directed by the Covered Entity, an Individual such Protected Health Information contained in a Designated Record Set. In the event any Individual requests access to Protected Health Information directly from Business Associate, Business Associate shall within five (5) days forward such request to the Covered Entity. Any denials of access to the Protected Health Information requested shall be the responsibility of the Covered Entity.
- e) Amendment of Protected Health Information. Within fifteen (15) days of receipt of a request from the Covered Entity or an Individual for the amendment of Protected Health Information or a record regarding an Individual contained in a Designated Record Set, Business Associate shall provide such information to the Covered Entity for amendment and incorporate any such amendments in the Protected Health Information as required by 45 C.F.R. Section 164.526. It shall be the Covered Entity's responsibility to promptly notify Business Associate of the request for an amendment. Any denials, in whole or in part, of requested amendments shall be done in accordance with 45 C.F.R. Section 164.526 and shall be the responsibility of the Covered Entity.
- f) Disclosure Accounting. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. Within fifteen (15) days of receipt of notice from the Covered Entity that it has received a request for an accounting of disclosures of Protected Health Information regarding an individual during the six (6) years prior to the date on which the accounting was requested, Business Associate shall make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. Section 164.528. At a minimum, Business Associate shall provide the Covered Entity with the following information: (1) the date of the disclosure; (2) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person; (3) a brief description of the Protected Health Information disclosed; and, (4) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. It shall be the Covered Entity's responsibility to promptly notify Business Associate of the request for an accounting, and to prepare and deliver any such accounting requested. Business Associate hereby agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this section.
- g) Access to Business Associate's Internal Records. Business Associate will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered

Entity available to the Covered Entity or the Secretary, for the purposes of the Secretary's determining Covered Entity's compliance with the Privacy Rule.

- h) Return of Protected Health Information. Business Associate shall at the termination of this Agreement with Covered Entity, if feasible, return or destroy all Protected Health Information received from, or created or received by Business Associate on behalf of, the Covered Entity that Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protection of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- i) Electronic Transactions. In the event the Business Associate transmits or receives any Covered Electronic Transaction on behalf of the Covered Entity, it shall comply with all applicable provisions of the Standards for Electronic Transactions Rule to the extent Required by Law, and shall ensure that any agents and subcontractors that assist Business Associate in conducting Covered Electronic Transactions on behalf of the Covered Entity agree in writing to comply with the Standards for Electronic Transactions Rule to the extent Required by Law.

2.5 **Obligations of Covered Entity.**

- a) Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R. 164.520, as well as any changes to such notice.
- b) Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rules if done by Covered Entity. This includes, but is not limited to, requests for disclosure of Protected Health Information to the sponsoring employer as other than the entity acting on behalf of the Plan as the Covered Entity. To the extent a dispute or difference of opinion exists between the Business Associate and the sponsoring employer as the entity acting on behalf of the Plan as the Covered Entity, Business Associate may disclose under objection pursuant to the specific, written direction of the Covered Entity. Any disclosures made pursuant to such specific, written direction shall be subject to the indemnification provisions of the Agreement.
- (c) Changes in Permission. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- (d) Restrictions. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

SECTION 3 – TRADING PARTNER PROVISIONS

- 3.1 **Introduction.** This Section 3 applies only if and to the extent that Business Associate and Covered Entity conduct electronic transactions that are subject to Standards for Electronic Transactions Rule. The Business Associate may be considered a "trading partner" of the Covered

Entity under the Standards for Electronic Transactions Rule. This Section 3 will govern the terms and conditions under which Covered Electronic Transactions are conducted.

3.2 **Mutual Obligations.** The mutual obligations of the Covered Entity and Business Associate include the following:

- a) EDI Data Transmission Accuracy. The parties will take reasonable care to ensure that Data Transmissions are timely, complete, accurate and secure.
- b) Retransmission of Lost or Indecipherable Transmissions. A party will retransmit the original transmission within two (2) business day(s) of its discovery that a Data Transmission is a Lost or Indecipherable Transmission.
- c) Equipment Cost. Each party will obtain and maintain, at its own expense, its own Operating System necessary for timely, complete, accurate and secure Data Transmission pursuant to this Agreement.
- d) Transmission Format. All standard transactions, as defined by Social Security § 1173(a) and the Standards for Electronic Transactions Rule, conducted between the Covered Entity and Business Associate, will only use code sets, data elements and formats specified by the Standards for Electronic Transactions Rule.
- e) Backup Files. Each party will maintain adequate backup files, electronic tapes or other sufficient means to recreate a Data Transmission for at least six (6) years from the Data Transmission's creation date.
- f) Testing. Prior to the initial Data Transmission, each party will test and cooperate with the other party in testing each party's Operating System to ensure the accuracy, timeliness, completeness and confidentiality of each Data Transmission.
- g) Data and Data Transmission Security. The Covered Entity and Business Associate will employ security measures necessary to protect Data and Data Transmissions between them in compliance with Social Security Act § 1173(d) and any HHS implementing regulations or guidelines.
- h) Security Access Codes. The Security Access Codes that the Covered Entity issues to Business Associate will, when affixed to Data Transmissions, be legally sufficient to verify the identity of the transmitter and to authenticate the Data Transmission, thereby establishing the Data Transmission's validity.

- 3.3 **Business Associate Obligations.** Business Associate will:
- a) Use Data only according to the terms of this Agreement.
 - b) Protect and maintain the confidentiality of Security Access Codes issued to Business Associate by the Covered Entity.
 - c) Limit disclosure of Security Access Codes to authorized personnel on a need-to-know basis.
- 3.4 **The Covered Entity's Obligations.** The Covered Entity will:
- a) Make available to Business Associate, via electronic means, Data and Data Transmissions for which this Agreement grants Business Associate access or authorization, or as provided by law;
 - b) Provide Business Associate with Security Access Codes that will allow Business Associate access to the Plan's Operating System. The Covered Entity reserves the right to change Security Access Codes at any time and in such a manner as the Covered Entity, in its sole discretion, deems necessary.
- 3.5 **Confidentiality and Security.**
- a) Data Security. Business Associate will maintain adequate security procedures to prevent unauthorized access to Data, Data Transmissions, Security Access Codes, Envelope, backup files, Source Documents or the Covered Entity's Operating System. Business Associate will promptly notify the Covered Entity of any unauthorized attempt to obtain access to or otherwise tamper with Data, Data Transmissions, Security Access Codes, Envelope, backup files, Source Documents or the Covered Entity's Operating System.
 - b) Operating Systems Security. Each party will develop, implement and maintain measures necessary to ensure the security of each party's own Operating System and each party's records relating to it Operating System and in compliance with applicable law.
- 3.6 **Records Retention and Audit.**
- a) Records Retention. Business Associate will maintain complete, accurate and unaltered copies of all Source Documents from all Data Transmissions it receives from the Covered Entity for not less than six (6) years from the date that Business Associate receives them. All retained records will be subject to the same security measures as Data and Data Transmissions.
 - b) Trade Data Log. The Covered Entity and Business Associate will each establish and maintain a Trade Data Log to record all Data Transmissions between the parties during the term of this Agreement. Each party will take necessary and reasonable steps to ensure that its Trade Data Log constitutes a complete, accurate, and unaltered record of each Data Transmission between the parties. Each party will retain Data Transmission records for not less than six (6) month(s) following the date of a Data Transmission. Each party will maintain its Trade Data Log on electronic media or other suitable means that permit timely retrieval and presentation in readable form.

SECTION 4 – ELECTRONIC SECURITY PROVISIONS

- 4.1 **Introduction.** This Section 4 applies only if and to the extent electronic data will be exchanged between the Business Associate and Covered Entity. The Business Associate may be considered a Business Associate of the Covered Entity under HIPAA, 45 CFR Part 142 (the "Security Regulations"). This Section 4 will govern the terms and conditions under which electronic data is exchanged.
- 4.2 **Security Regulations.** In accordance with the Security Rule as it exists at the time of this Agreement, Business Associate agrees to:
- a) Implement administrative, physical and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic Protected Health Information that it creates, maintains or transmits on behalf of the Covered Entity;
 - b) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
 - c) Report to the Covered Entity any Security Incident of which it becomes aware;
 - d) Authorize termination of the Agreement if the Covered Entity determines that the Business Associate has violated a material term of the Agreement.
- 4.3 **Subsequent Modifications.** In recognition that the Security Regulations are not effective until twenty-four (24) months following publication of the final regulations, Business Associate agrees this Agreement shall be amended as necessary to comply with the final Security Regulations, any such changes to be subsequently incorporated into this Agreement as Exhibit A.

SECTION 5 – TERM AND TERMINATION

- 5.1. **Term.** The Term of this Agreement will begin and become effective on the compliance date applicable to Covered Entity under the Privacy Rule, and shall terminate when all of the Protected Health Information created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Paragraph 5.1.
- 5.2 **Termination.** In the event that Covered Entity discovers and determines that Business Associate materially breached or violated any of its obligations under this Agreement, Covered Entity will notify Business Associate of such breach in writing. Covered Entity may terminate the Agreement or may provide Business Associate with an opportunity to take reasonable steps to cure the breach or end the violation, as applicable, within a mutually agreed upon period of time. If Covered Entity's attempts to cure the breach or end the violation are unsuccessful within that period without limiting the rights of the parties under the Agreement, Covered Entity may terminate the Agreement.
- 5.3 **Effect of Termination.**

- a) Except as provided in paragraphs (b) and/or (c) of this sub-section, upon termination of the Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information created or received by it on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of Business Associate and/or its subcontractors or agents. Business Associate will not retain any copies of Protected Health Information.
- b) In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate will notify Covered Entity of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of Protected Health Information is infeasible, Business Associate will extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.
- c) Should the Covered Entity notify Business Associate that the information necessary to comply with the recordkeeping requirements under other applicable law including, but not limited to, the Employee Retirement Income Security Act of 1974 ("ERISA"), includes the Protected Health Information, Business Associate shall return or provide to Covered Entity such information, including Protected Health Information.

SECTION 6 – GENERAL PROVISIONS

- 6.1 Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- 6.2 Amendment.** The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- 6.3 Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.
- 6.4 Survival.** The respective rights and obligations of Business Associate and the Covered Entity shall under this Agreement survive the termination of this Agreement and any related Services Agreement.

6.5 **Permissible Requests by Covered Entity.** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except as otherwise provided herein.

6.6 **Indemnity.** Business Associate will indemnify and hold harmless Covered Entity and Covered Entity's affiliates, officers, directors, employees or agents from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted or violating use or disclosure of Protected Health Information or other breach of this Agreement by Business Associate or any subcontractor, agent, person or entity under Business Associate's control.

6.7 **Conformance with Law.** Upon the effective date of any final regulation or amendment to final regulations promulgated by the U.S. Department of Health and Human Services with respect to Protected Health Information or Covered Electronic Transactions, this Agreement will automatically amend such that the obligations they impose on the Business Associate remain in compliance with these regulations.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date set forth below.

Covered Entity:

This _____ day of _____, _____

By: _____

on behalf of the <<name of plan>>, a Covered Entity

Print Name: _____

Title: _____

Business Associate:

This _____ day of _____, _____

Company Name: _____

By: _____

Print Name: _____

Title: _____

Retention of PHI Documentation

Policy Statement

The Health Plan shall maintain all protected health information (PHI) documentation for a period of at least six (6) years from the date of its creation, or the date on which the document was last in effect, whichever is later.

Policy Interpretation and Implementation

Retention of PHI Documents

1. Certain documents classified as "privacy related documents" must be maintained for a period of at least six (6) years from the date of creation, or the date on which the document was last in effect, whichever is later.

Privacy Related Documents

2. "Privacy related documents" include:
 - a. Documentation that identifies the:
 - i. Name, telephone number and address of the Health Plan's HIPAA Privacy Officer;
 - ii. Name, title, telephone number and address of the individual responsible for receiving complaints;
 - iii. Name, title, telephone number and address of the individual responsible for obtaining and processing access, use, and disclosure of PHI requests;
 - iv. Name, title, telephone number and address of the individual responsible for receiving and processing amendment of PHI requests;
 - v. Attempts to obtain consent when consent could not be obtained and the reason(s) why such consent could not be obtained;
 - vi. Method by which PHI will be de-identified;
 - vii. Sanctions imposed against Health Plan employees, business associates, or others who violate Health Plan policy/HIPAA regulations;
 - b. All signed authorizations, consents, and agreed to restrictions;
 - c. Copies of all notices of privacy practices (NPPs) including any revisions to such NPPs;
 - d. Accounting of disclosures logs;
 - e. Any privacy complaints received and their dispositions; and
 - f. Copies of all HIPAA related policies and

procedures.

**Adding/Deleting
Documentation**

3. Documents may be added or deleted from the above listing as may become necessary by law or as may be established by Health Plan practice or policy.

**Identifying/Storage of PHI
Documents**

4. The HIPAA Privacy Officer is responsible for identification and storage of privacy related records, electronic files, etc., for purposes of complying with this policy.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

6. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

7. Violations of this policy will be subject to discipline.

Effective Date

8. April 14, 2004.

References:

45 C.F.R. § 164.530(j)

HIPAA Privacy Training Program

Policy Statement

The Health Plan must train all relevant members of its workforce on HIPAA policies and procedures, as necessary and appropriate for the members of the workforce to carry out their function within the Health Plan.

Policy Interpretation and Implementation

HIPAA Training Program

1. To ensure the confidentiality of individual's protected health information (PHI), HIPAA training (HIPAA Training) shall be provided for all employees of the Plan Sponsor who have responsibilities involving the use/disclosure of PHI, and other workforce members as deemed necessary within the sole discretion of the HIPAA Privacy Officer. It is the HIPAA Privacy Officer's responsibility to oversee such HIPAA Training.

Workforce Members

2. An employee/workforce member, for the purposes of this policy, means any employee, trainee, volunteer, , or any other person(s) whose conduct, in the performance of work for the Health Plan, is under the direct control/supervision of the Health Plan, regardless of payment source.

Content of HIPAA Training Program

3. The HIPAA Training shall include, but is not limited to:
 - a. An overview of the HIPAA privacy regulations relative to the identification and protection of PHI.
 - b. A review of the Health Plan's HIPAA policies and procedures;
 - c. Permissible uses and disclosures of PHI;
 - d. Application of the Health Plan's HIPAA policies and procedures to employee's job responsibilities;
 - e. The identity and location of the Health Plan's HIPAA Privacy Officer;
 - f. The requirement that all employees report any potential violations of the Health Plan's policies and procedures or the HIPAA regulations, whether caused by a workforce member or a service provider, to the HIPAA Privacy Officer; and
 - g. Other information relative to the protection and security of PHI.

**Newly Hired Employees/
Business Associates**

4. Before being allowed access to PHI, all newly hired employees, and employees new to a position requiring access to PHI, shall be required to sign and date a written acknowledgement that the new employee has completed HIPAA Training.

**Acknowledgment of Training
Attendance**

5. Department directors will be required to have a signed and dated written acknowledgment that the new employee has completed HIPAA Training before being allowed access to PHI.

Attendance Records

6. The HIPAA Privacy Officer shall maintain a record of all personnel who attend HIPAA Training. Such records shall be maintained in accordance with the *Retention of PHI Documentation Policy*.

Annual Training

7. Updated training shall take place at least annually. Should a change in the training program or security systems occur before an annual training session occurs, impacted employees shall receive interim training materials or abbreviated instructions.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. April 14, 2004.

References:

45 C.F.R. § 164.530(b)

ACKNOWLEDGMENT OF TRAINING ATTENDANCE

Please note: This Administrative Form relates to the Health Plan's Policy Form 17, HIPAA Privacy Training Program.

I, _____, acknowledge that I have attended and completed HIPAA Training on _____, 200__.

Name (print)

Signature

Date

Personal Representative

Policy Statement

The Health Plan must treat a personal representative the same as it would the individual who is the subject of the protected health information (PHI), unless one of the exceptions applies. In general, a personal representative is someone who is recognized under applicable state law as a personal representative (e.g., parent/guardian, power of attorney, executor of estate).

Policy Interpretation and Implementation

Designation as Personal Representative

1. The person who is the subject of the PHI may designate another person as a personal representative, or a person may seek to be recognized as a personal representative, by filing the appropriate written documentation with the Health Plan.

Rights of Personal Representative

2. The personal representative must be treated the same as the individual, except as specified below:

Restrictions on Personal Representative

- a. If the Health Plan reasonably believes that the individual has been or may be subjected to domestic violence, abuse, or neglect by the person seeking to be treated as a personal representative, or that treating the person as the personal representative could endanger the individual.
- b. If the Health Plan, in the exercise of professional judgment, decides that treating the person as the individual's personal representative would not be in the individual's best interest.
- c. If a parent is the personal representative of a minor child, but disclosure to the parent is prohibited under state law.
- d. If a minor child consented to the treatment, no other consent was required, and the minor has not requested the person be treated as the minor's personal representative.
- e. If a minor child may lawfully obtain treatment without the consent of a parent and consent was lawfully obtained.
- f. If the parent has agreed to a confidential relationship between the minor and the physician with respect to that treatment.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

5. Violations of this policy will be subject to discipline.

Effective Date

6. April 14, 2004.

References:

45 C.F.R. § 164.502(g)

DESIGNATION OF PERSONAL REPRESENTATIVE FORM

Please note: This Administrative Form relates to the Health Plan's Policy Form 18, Personal Representative.

Note: This form is used to confirm permission for the Health Plan to discuss with or disclose to a person's protected health information ("PHI") to a particular individual who acts as the person's personal representative. Use of this information is strictly limited to that purpose.

Subject of PHI's Name: _____ Date: _____

Please complete either Part I or Part II below.

PART I: DESIGNATION BY SUBJECT OF PHI

I hereby authorize the following person to act as my personal representative as indicated below. I understand that this authorization is voluntary and that I may revoke this authorization at any time except to the extent that action has been taken in reliance on this authorization.

Name of personal representative: _____

Date of birth of personal representative (used for verification purposes on phone inquiries): _____

Social Security # of personal representative (used for verification purposes on phone inquiries): _____

Address: _____

Relationship to me: _____

Password personal representative must provide to access protected health information ("PHI") about me:

Password: _____

Description of nature of representation and limits thereon (attach supporting documentation, if any, such as court orders, Power of Attorney, etc): _____

NOTE: I understand that I have the right to limit the information that is released under this authorization. For example, I may limit my personal representative's access to information about a particular issue. Any such limitations must be described below in writing. I understand that by leaving this section blank, I am imposing no limitations on disclosure.

Limitations on Disclosure:

I understand that I may revoke this authorization at anytime by providing written notice of such revocation to the Health Plan.

I have had full opportunity to read and consider the content of this Designation of Personal Representative form. I confirm that this authorization is consistent with my request. I understand that, by

signing this form, I am confirming my authorization that the Health Plan may use and/or disclose my PHI to the person named as personal representative for the purpose described above.

Date: _____	Signature: _____
	Printed name: _____
Date: _____	Signature of witness: _____
	Printed name of witness: _____

PART II: THIRD PARTY DESIGNATION

Name of personal representative: _____

Date of birth of personal representative (used for verification purposes on phone inquiries): _____

Social Security # of personal representative (used for verification purposes on phone inquiries): _____

Address: _____

Relationship to Subject of PHI: _____

Password personal representative must provide to access protected health information ("PHI") about me:

 Password: _____

Description of nature of representation and limits thereon (attach supporting documentation, if any, such as court orders, Power of Attorney, etc): _____

For office use only:

Received by: _____ Date: _____

Coordination with Other Laws

Policy Statement

In addition to being subject to HIPAA, the Health Plan may also be subject to other state and federal laws regarding medical information and privacy. The Health Plan intends to comply with all applicable state and federal laws. However if there is a conflict between the laws, the HIPAA Privacy Officer will resolve the conflict according to this Coordination with Other Laws policy.

Policy Interpretation and Implementation

Floor

1. The HIPAA regulations are the floor above which other laws may create more narrow restrictions. No law, whether federal or state, may allow less restriction than HIPAA.

Apply Both Laws

2. If a potential conflict exists, the Health Plan shall attempt to find a way to comply with both laws. For example, if one law permits disclosure, but HIPAA does not, the Health Plan could obtain an individual authorization and succeed in complying with both laws.

Follow the Law that Requires Use or Disclosure

3. If another federal law *requires* disclosure or use of PHI that HIPAA prohibits, the Health Plan may use or disclose the PHI in accordance with the other federal law. This is not a violation of HIPAA. HIPAA's privacy rules allow the Health Plan to use or disclose PHI as required by other federal laws.

Follow the More Specific Law

4. If there is a very specific law regarding use or disclosure of PHI that is in conflict with HIPAA, the more specific law should be followed. For example, if HIPAA allows an individual a right to access test results, but a specific federal law prohibits that type of disclosure, the specific law should be followed.

State Law Preemption

5. HIPAA provides for preemption of state laws that are less restrictive than HIPAA. However, HIPAA does not preempt state laws that are more restrictive. If the Health Plan encounters a conflict between HIPAA and a state law, the Health Plan should follow the more restrictive law.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. April 14, 2004.

References:

Preamble to HIPAA Regulations

Disclosures to Plan Sponsor

Policy Statement

The Health Plan may not disclose protected health information (PHI) to the plan sponsor except in specific situations recognized by HIPAA.

Policy Interpretation and Implementation

Definition of Plan Sponsor

1. The term "plan sponsor" means (i) the employer in the case of an employee benefit plan established or maintained by a single employer, (ii) the employee organization in the case of a plan established or maintained by an employee organization, or (iii) in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.

Permitted Disclosure to Plan Sponsor for Settlor Functions

2. Summary health information may be disclosed to the plan sponsor for:
 - a. Obtaining premium bids for providing health insurance coverage under the Health Plan; and
 - b. Modifying, amending or terminating the Health Plan.

Summary Health Information

3. Summary health information is information that summarizes the claims history, expenses, or types of claims by individuals for whom the Plan Sponsor has provided health benefits under the Health Plan.

Permitted Disclosure to Plan Sponsor for Plan Administration Functions

4. To the extent described in the plan documents and notice of privacy practices, the Health Plan may disclose PHI to the plan sponsor necessary to perform plan administration activities such as:
 - a. Quality assurance;
 - b. Claims processing;
 - c. Auditing; and
 - d. Monitoring and managing carve-out plans like vision and dental.

Enrollment Functions

5. These restrictions do not affect the plan sponsor's ability to perform enrollment functions on behalf of its employees.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. April 14, 2004.

References:

45 C.F.R. § 164.504(f)

Duty to Mitigate

Policy Statement

The Health Plan will mitigate, to the extent practicable, any harmful effect that is known to the Health Plan of a use or disclosure of protected health information (PHI) in violation of its policies and procedures by the Health Plan or its business associates.

Policy Interpretation and Implementation

Mitigation Actions

1. When a violation of the Health Plan's policies and procedures are brought to the attention of the Health Plan, the following action will be taken:
 - a. The Privacy Officer will be notified and will start an immediate investigation into the violation;
 - b. The Health Plan will identify the extent of the breach and will take reasonable steps to mitigate or correct the violation; and
 - c. The Health Plan will document the steps taken to mitigate.

Record Retention

2. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

3. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the Privacy Officer at 651-452-1850.

Violations

4. Violations of this policy will be subject to discipline.

Effective Date

5. April 14, 2004.

References:

45 C.F.R. § 164.530(f)

Discipline Policy

Policy Statement

HIPAA requires the Health Plan to discipline individuals subject to but who fail to comply with HIPAA's requirements as reflected in the Health Plan's privacy policies and procedures. The purpose of this Discipline Policy is to establish guidelines for the disciplinary processes.

<p>Please note: This Discipline Policy applies exclusively to violations of the Health Plan's privacy policies and procedures.</p>

Policy Interpretation and Implementation

Discipline Policy

1. A failure to comply by an individual subject to the Health Plan's policies and procedures, or with the provisions of HIPAA, will be addressed in a timely manner. Specific disciplinary actions to be taken will be proportional to the severity of the infraction.

Initial Determination

2. The HIPAA Privacy Officer, in its sole discretion, shall make an initial determination, if true, the allegations in the complaint constitute a violation of the Health Plan's privacy policies and procedures.

Discipline Procedure

3. Complaints or allegations against an individual will be discussed with the individual in question by the HIPAA Privacy Officer and, if deemed appropriate, will be investigated by the HIPAA Privacy Officer.
4. In general, a known or intentional infraction of the Health Plan's policies and procedures, or of HIPAA's provisions, will result in:
 - a. First offense: Oral counseling by the HIPAA Privacy Officer, and written documentation in the individual's file.
 - b. Second offense: Oral counseling by the HIPAA Privacy Officer, and a written warning.
 - c. Third offense: Discipline up to and including probation, suspension or termination of employment.

Intentional Misuse

5. In general, intentional misuse or abuse of PHI will result in:
 - a. First offense: Oral counseling by the HIPAA Privacy Officer, and written documentation in the individual's file.
 - b. Second offense: Oral counseling by the HIPAA Privacy Officer, and a written warning.

- c. Third offense: Discipline up to and including probation, suspension or termination of employment.
- 6. Notwithstanding items 4 and 5, the HIPAA Privacy Officer retains discretion to deviate based on the particular facts and circumstances. Each infraction will be handled on an individual basis to ensure that disciplinary actions are proportional to the severity of the infraction.
- 7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.
- 8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.
- 9. April 14, 2004.

Record Retention

HIPAA Privacy Officer

Effective Date

References:

45 C.F.R. § 164.530(e)

Administrative Safeguards

Policy Statement

The Health Plan will make reasonable efforts to maintain adequate administrative, technical and physical safeguards to protect the privacy of protected health information (PHI) from unauthorized use or disclosure, whether intentional or unintentional, and from theft and unauthorized alterations.

Policy Interpretation and Implementation

Implementation of Safeguards

1. The HIPAA Privacy Officer will work with appropriate personnel to determine and implement safeguards to protect PHI from unauthorized use or disclosure.

Periodic Review

2. The HIPAA Privacy Officer will complete periodic reviews with all business units regarding the transportation, storage, usage, disclosure, and disposal of PHI to identify risks to the privacy and security of the PHI. If necessary, policies and procedures will be amended and the applicable workforce retrained in order to maintain reasonable efforts of safeguarding such information.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

4. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. If you have a question or concern about your HIPAA rights contact the Privacy Officer at 651-452-1850.

Violations

5. Violations of this policy will be subject to discipline.

Effective Date

6. April 14, 2003.

References:

45 C.F.R. § 164.530

Computer Terminals/Workstations

Policy Statement

Computer terminals and workstations will be positioned/shielded to ensure that protected health information (PHI) is protected from public view, view by those without a need to know whether inadvertent or otherwise, or unauthorized access.

Policy Interpretation and Implementation

Positioning/Shielding Workstation/Terminals

1. Insofar as practical/feasible, computer terminals/workstations shall be positioned or shielded so that screens are not visible to the public and/or to unauthorized staff.

Access Limitations

2. Only authorized users are granted access to individual and Health Plan information. Such access is limited to specific, denied, documented and approved applications and level of access rights.

Leaving Workstations or Terminals Unattended

3. A user may not leave his/her workstation or terminal unattended for long periods of time (e.g., breaks, lunch, meetings, etc.) unless the terminal screen is cleared and the user is logged off. Each user must log off at the end of his/her work shift.

Clearing Terminal Screens

4. A user must clear the terminal screen if the workstation or terminal is left briefly unattended.

Securing Hard Copy Data

5. All hard copy printed information must be positioned in such a manner that it cannot be viewed or read by the public and/or unauthorized staff. Such data must be placed in designated secure areas upon leaving the work area and at the end of the work shift.

Sharing/Piggyback of Password/User ID Code

6. A user may not (1) share or disclose his/her password or ID code with other staff members or other non-staff members, or (2) allow staff members or other non-staff members access privileges (e.g., piggyback access) while the user is logged onto the information system used by the Health Plan.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

8. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about

HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. April 14, 2004.

References:

See generally 45 C.F.R. § 164.530

Electronic Mail System (E-Mail)

Policy Statement

The Health Plan utilizes electronic mail (E-Mail) in transmitting individual and Health Plan information. Established security measures must be followed by all personnel who have the authority to access, use, or transmit protected health information (PHI) electronically.

Policy Interpretation and Implementation

Application of Policies

1. This policy applies to all usage of e-mail systems related to the Health Plan whether or not the e-mail is originated from or is received into the computer or network system used by the Health Plan. Such policies apply to all authorized users including employees, business associates, staff or consultants.

Definition of Authorized User

2. For the purposes of this policy, an "authorized user" is defined as any person who (1) has been assigned a password and user ID code and (2) has the authority to read, enter, or update information created or transmitted by the Health Plan.

Personal Use or E-Mail and Internet Systems

3. Users have the responsibility and obligation to use e-mail and internet systems appropriate, effectively, and efficiently. Incidental personal use is permissible if:
 - a. Personal use is limited to meal and break times;
 - b. It does not interfere with the normal business use of such services;
 - c. It does not interfere with the work productivity of the user or other employees; and
 - d. Passwords and user ID codes are not shared with others.

Improper Use of Health Plan's E-Mail or Internet Services

4. Improper use of e-mail and internet services is strictly prohibited. Examples of such improper use include, but are not limited to:
 - a. Sending/forwarding harassing, insulting, defamatory, obscene, offending or threatening messages;
 - b. Gambling, surfing or downloading pornography;
 - c. Downloading or sending confidential individual or PHI without proper authorization;
 - d. Copying or transmission of any document,

software or other information protected by copyright and/or patent law, without proper authorization;

- e. Transmission of highly sensitive or confidential information (e.g., HIV status, mental illness, chemical dependency, workers' compensation claims, etc.);
- f. Obtaining access to files or communication of others without proper authorization;
- g. Attempting unauthorized access to individual or Health Plan data;
- h. Attempting to breach any security measure on any of the Health Plan's electronic communication system(s);
- i. Attempting to intercept any electronic communication transmission without proper authorization;
- j. Misrepresenting, obscuring, suppressing, or replacing an authorized user's identity;
- k. Using e-mail addresses for marketing purposes without permission from the recipient(s);
- l. Using e-mail system for solicitation of funds, political messages, or any other illegal activities; and/or
- m. Releasing of passwords and user ID codes.

Ownership of E-Mail Messages

- 5. Messages whether originated or received into the Health Plan e-mail system are considered to be the property of the Health Plan and, therefore, are subject to the review and monitoring of the HIPAA Privacy Officer. The Health Plan reserves the right to access employee e-mail (whether present or not) for the purposes of ensuring the protection of individual/Health Plan information.

Inadvertent Access to E-Mail

- 6. During routine maintenance, upgrades, problem resolution, etc. information systems technician(s) may inadvertently access user e-mail communications. Such staff, when carrying out their assignments, will not intentionally read or disclose content of e-mail unless such data is found to be in violation of the HIPAA Policies and Procedures.

Protection of Information

- 7. Users of the e-mail system must ensure that all information forwarded, distributed, or printed is protected according to the HIPAA Policies and Procedures.

Responding to E-mail Messages

8. When an e-mail message is received containing PHI, any reply of response to that message (i.e., an acknowledgement or receipt of the message) must not include PHI. E-mail systems often automatically include the sender's e-mail message when a reply is made. When the original message includes PHI, the function of the software must be disabled or the original message must be manually deleted prior to sending a reply.

Maintaining/Archiving E-Mail Messages

9. E-mail messages may not be maintained or archived for more than thirty (30) days, unless otherwise approved by the HIPAA Privacy Officer.

Record Retention

10. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

11. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The HIPAA Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. If you have a question or concern about your HIPAA rights contact the HIPAA Privacy Officer at 651-452-1850.

Violations

12. Violations of this policy will be subject to discipline.

Effective Date

13. April 14, 2004

References:

See generally 45 C.F.R. § 164.530

Facsimile Machines

Policy Statement

The Health Plan utilizes facsimile (fax) machines to transmit data from one location to another on a routine basis. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the transmission or receipt of data via a facsimile machine. This policy outlines the required elements for a secure location of a facsimile machine. The procedure establishes guidelines for how the Health Plan will reasonably safeguard the transmission and receipt of PHI via a facsimile machine to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Secure Location

1. Fax machines used to transmit or receive PHI shall be placed in secure locations. Whenever possible, fax machines used to receive PHI will not be used regularly for other purposes.

Pre-Programmed Numbers

2. Frequently used destination numbers will be pre-programmed into fax machines and tested before being used to transmit PHI. Each fax machine will display a key that identifies the destination for each pre-programmed fax number.

Non Pre-Programmed Numbers

3. When PHI is faxed to a destination number that is not pre-programmed, the fax machine operator will double-check the accuracy of the number in the machine's display before sending the fax.

Cover Letter

4. All fax messages will include a standard cover sheet, developed by the Privacy Officer, with the following (or substantially similar) statement:

Confidentiality Statement: The documents accompanying this transmission contain confidential health information that is legally privileged. This information is intended only for the use of the individuals or entities listed above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

Transmittal Sheets

5. Transmittal sheets will be checked immediately after each transmission of PHI, to assure that the information was sent to the correct number.

Misdirected Faxes

6. If PHI has been sent to the wrong fax number, the sender must immediately send a second fax to the

number that was contacted in error, reiterating the confidentiality message, and asking the recipient to telephone the sender immediately to arrange proper disposition of the information. Any instance of transmitting PHI to the wrong destination number must be reported to the Privacy Officer immediately. The report must include the date, time, the wrong number, the correct number, the intended recipient, the identity of the member, and a brief description of the information that was transmitted in error. Transmission of PHI by fax to a wrong number must be included in an accounting of disclosures of PHI.

Received Faxes

7. Prior to distribution of a received fax message, the fax message must be reviewed to make sure that all pages that belong to that fax message have been received and are together, and pages that belong to other fax messages are not included. The cover sheet received with the message, if any, will be placed on top of the message.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

9. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the Privacy Officer at 651-452-1850.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. April 14, 2004.

References:

See generally 45 C.F.R. § 164.530

Copy Machines

Policy Statement

The Health Plan utilizes copy machines to copy data on a routine basis. The Health Plan also occasionally utilizes third party copy services to copy data. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the copying of data. This policy outlines the required elements for a secure location of a copy machine and establishes guidelines for how the Health Plan will reasonably safeguard PHI during copying to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Secure Location

1. Copy machines used to copy PHI shall be placed in secure locations. Whenever possible, copy machines used to copy PHI will not be used regularly for other purposes.

Removal of Original

2. Following the copying of any document containing PHI, the person making the copies will double-check to confirm that no original documents containing PHI are left on or at the copy machine.

Removal of Copies

3. Following the copying of any document containing PHI, the person making the copies will double-check to confirm that none of the copies containing PHI are left on or at the copy machine.

Erasing Memory

4. If the copy machine is equipped with a memory that allows the reprinting of a document previously copied, upon completion of the copy job involving documents containing PHI, the person making the copies will delete the memory and double-check that the memory has been deleted prior to leaving the copy machine.

Destruction of Certain Copies

5. In the event a copy containing PHI is unusable (because it is not dark enough, etc.) and is to be destroyed, the person making the copy will destroy the copy, regardless of whether it is legible, by shredding it.

Unattended Copying

6. In no instance shall the person making copies of documents containing PHI leave the copier unattended while copies are being made.

Outsourcing

7. To the extent possible, copies of PHI should be made on site in accordance with the foregoing procedures. In some instances it may, however, be appropriate to outsource copying of documents and data containing PHI to a third party copy service (i.e., large volumes of documents to copy or large numbers of copies needed). Prior to providing

documents/data containing PHI to any such copy service for copying, the copy service must sign a business associate agreement. Furthermore, the Mail policy shall be followed with respect to delivering the original documents/data to the copy service.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

9. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the Privacy Officer at 651-452-1850.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. April 14, 2004.

References:

See generally 45 C.F.R. § 164.530

Mail – Internal and External

Policy Statement

The Health Plan utilizes both internal and external mail (i.e., postal service and delivery services) to deliver data on a routine basis. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the mailing of data. This procedure establishes guidelines for how the Health Plan will reasonably safeguard PHI during mailing of data to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Addresses

1. When PHI is mailed, whether internally or externally, the person sending the mail will double-check the accuracy of the address of the addressee before sending the mail.

Information Contained on Envelopes

2. When PHI is mailed, whether internally or externally, no PHI shall be included on the envelope, nor shall it be visible through the envelope, including any window in the envelope. With respect to internal mail, only the recipients name shall be indicated on the envelope.

Secure Envelopes

3. When PHI is mailed, whether internally or externally, it should be mailed in a sealed envelope or an envelope that may be securely closed and it should not be provided to unauthorized staff or third persons (i.e., mail room staff) until properly sealed or closed. To the extent it is impractical to place it in a secure envelope, interoffice mail may be transmitted without an envelope, provided that the first page of the mail does not contain PHI (i.e., a cover page is used or the first page is turned over) and PHI is not otherwise visible.

Receipt of Mail

4. Only authorized staff shall open mail that is received, whether from internal or external sources, from a subject of PHI or from any other party where it is likely the mail contains PHI. To the extent mail is received in an envelope that is not addressed to a specific person, where it is unclear that it is from the subject of PHI, or where it is unclear whether it may contain PHI, the mail may be opened by unauthorized staff, provided that person opening the envelope reviews the least amount of contents needed to determine to whom the mail is addressed and/or that it contains PHI, at which time the mail should be delivered to the appropriate person.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or

electronic format, or both.

Privacy Officer

6. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the Privacy Officer at 651-452-1850.

Violations

7. Violations of this policy will be subject to discipline.

Effective Date

8. April 14, 2004.

References:

See generally 45 C.F.R. § 164.530

Storage of Documents

Policy Statement

Documents containing protected health information (PHI) will be stored so that they are protected from public view, view by those without a need to know whether inadvertent or otherwise, or unauthorized access.

Policy Interpretation and Implementation

Storage of Documents

1. Documents containing PHI shall be stored in locked file cabinets separate from other documents (i.e., personnel files) to which unauthorized staff may appropriately have access. Insofar as practical/feasible, the file cabinets shall be located in a secure location

Access Limitations

2. Only authorized staff are granted access to individual and Health Plan information. Such access is limited to specific, denied, documented and approved applications and level of access rights.

Leaving File Cabinet Unlocked and Unattended

3. Authorized staff may not leave file cabinets containing documents with PHI unlocked and unattended for long periods of time (e.g., breaks, lunch, meetings, etc.). File cabinets must be locked at the end of the work shift.

Sharing Key to File Cabinet

4. Authorized staff may not (1) provide the key the any file cabinet containing PHI documents to other staff members or other non-staff members, or (2) allow other staff members or other non-staff members access to said file cabinets.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

Privacy Officer

6. The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures. The Privacy Officer is also the contact person for any questions or complaints regarding HIPAA. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer at 651-452-1850.

Violations

7. Violations of this policy will be subject to discipline.

Effective Date

8. April 14, 2004.

References:

See generally 45 C.F.R. § 164.530