SECTION 3: Benefits

XVII. Health Insurance Portability and Accountability Act (HIPAA)

A. Purpose

The Health Insurance Portability and Accountability Act ("HIPAA") was enacted in 1996. The Department of Health and Human Services has issued privacy and security regulations that cover health plans and health care providers, including the City of Celina's (the "City") health plan ("Health Plan") and the Fire Department, which provides emergency health services (the "Fire Department"). Because the City has many other functions other than providing a health plan and emergency medical services, the City has designated itself as a hybrid entity. Therefore, no other departments but the Health Plan and the Fire Department of the City will be covered by the regulations. However, individual employees who are covered by the Health Plan have certain privacy rights because of the HIPAA regulations, as do patients cared for by the City's Fire Department. This policy is for the protection of those privacy rights.

B. Definitions

1. Protected health information ("PHI") is any individually identifiable health information that is transmitted or maintained in any form, including demographic information collected from an individual, and:
   a) Is created or received by one of the city's health care providers (medical, dental, vision) or the City; and
   b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   c) That identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual.
2. "Use" of PHI is the sharing, examining, or analysis of individually identifiable health information by any city employee or by a Business Associate of the City.
3. A "Business Associate" is an external agency, consultant, or individual who may send or receive PHI on the City's employees. A "business associate" must have on file a current agreement with the city stating the intent of that organization to comply with HIPAA requirements and in order to send or receive PHI relative to the city.

C. Responsibilities of the Privacy Officer

1. The Human Resources designee is designated as the City's Privacy Officer for the Health Plan. The Emergency Medical Services Chief is designated as the City's Privacy Officer for the Fire Department. Any questions about privacy policies and procedures should be directed to the Privacy Officer noted herein. Also, any complaints about the violation of this policy or your rights as described in our notice should be directed to the Privacy Officer or may be made to the Department of Health and Human Services at: U.S. Department of Health & Human Services, Office of Civil Rights, 200 Independence Avenue, S.W., Washington, D.C., 20201.
2. The Health Plan Privacy Officer is responsible for the following:
   a) Providing the *Notice of Privacy Policy* to all Health Plan participants (located in

the City of Celina Medical Plan document);

b) Posting the *Notice of Privacy Policy*, and all appropriate updates, in a prominent place and posting on the city's intranet page if made available to employees;
c) Processing all complaints and documenting all complaints related to HIPAA and the Health Plan, as well as the dispositions thereof.
d) Maintaining documentation of all complaints regarding privacy or other HIPAA violations for at least 6 years, or such other period as may be required by law.
e) Fulfilling statutory responsibilities as the Health Plan's Privacy Officer, including overall responsibility for the Health Plan's compliance with HIPAA, its related regulations and the Health Plan's privacy and security policies.
f) Ensuring that all of the Health Plan employees who have access to Protected Health Information ("PHI") by virtue of their job duties are periodically identified.
g) Selecting and ensuring implementation of an initial training program and then subsequent "new hire" training for all identified employees.
h) Ensuring that Business Associate Agreements are signed with any third parties to which the Health Plan gives PHI, and acting as the custodian for all Business Associate Agreements.
i) Monitoring compliance with the Health Plan's privacy and security policies including review to ensure that:
    (1) patients are given a Notice of Privacy Policy;
    (2) when PHI is used or disclosed to third parties, a signed Authorization to Use and Disclose Protected Health Information from the affected participant and that the disclosing employee complies with the Accounting of Disclosures Policy and placed a notation in the affected participant's file; and
    (3) PHI is not being used or disclosed to third parties except in accordance with Business Associate Agreements or for any reasons other than permitted by law.

3. Serving as a resource for the Health Plan's employees or participants with questions about privacy standards and practices and/or patients' rights.
4. Serving as the conduit for providing any documentation required when any participant asserts rights under HIPAA.
5. Monitoring legal and regulatory changes and suggest any needed policy and/or procedural changes.

D. Use and Disclosure of PHI

1. The City WILL require a valid authorization prior to requesting or using/disclosing PHI in certain required circumstances to another entity, health plan carrier, or as required to assist the employee or family member in researching health plan issues.
2. A HIPAA privacy authorization form is NOT required for any of the following:
    a) To carry out treatment, payment or health care operations by the plan as it relates to you or your covered family members;
    b) Drug testing or employment required testing or receipt of results;
    c) Workers' compensation claims processing or administration;
    d) American with Disabilities Act administration or related paperwork;
    e) Long Term Disability forms or inquiries;
    f) Life Insurance Claims, Forms, Insurability Questionnaires or Inquiries

g) For processing of normal daily activities such as payroll, documenting sick leave usage, sick leave donations, etc.

3. While the above list does not fall under HIPAA privacy rules, these areas are still handled under internal confidentiality rules and maintained in secured areas under the Human Resources designee's responsibility.

E. The Fire Department Privacy Officer is responsible for the following:
   1. Processing all complaints and documenting all complaints related to HIPAA and the Fire Department, as well as the dispositions thereof.
   2. Maintaining documentation of all complaints regarding privacy or other HIPAA violations for at least 6 years, or such other period as may be required by law.
   3. Fulfilling statutory responsibilities as the Fire Department's Privacy Officer, including overall responsibility for the Fire Departments compliance with HIPAA, its related regulations and the Fire Department's privacy and security policies.
   4. Ensuring that all of the Fire Department employees who have access to Protected Health Information ("PHI") by virtue of their job duties are periodically identified.
   5. Selecting and ensuring implementation of an initial training program and then subsequent "new hire" training for all identified employees.
   6. Ensuring that Business Associate Agreements are signed with any third parties to whom the Fire Department gives PHI, and acting as the custodian for all Business Associate Agreements.
   7. Serving as a resource for the patients or citizens with questions about privacy standards and practices and/or patients' rights.
   8. Serving as the conduit for providing any documentation required when any patient or citizen asserts rights under HIPAA.
   9. Monitoring legal and regulatory changes and suggest any needed policy and/or procedural changes.

F. Security Officer Responsibilities
   1. The Director of Information Technology is designated as the City's Security Officer. The Security Officer is responsible for technical controls in relation to the electronic transfer of PHI, including but not limited to network security, evaluating and protecting against external vulnerability, firewall protection, antivirus protection, etc. Any questions regarding electronic or information technology security related to the electronic transfer of PHI should be directed to the Security Officer.

G. Responsibilities of Covered Entities
   1. The Human Resources designee shall diligently protect the privacy of personally identifiable health information, unless the affected employee has waived his or her right of privacy under HIPAA. A HIPAA Authorization Form is available from Human Resources or the City Manager's Office.
   2. Human Resources will create administrative, technical, and physical safeguard procedures to appropriately protect the privacy of personally identifiable health information. Those safeguards must reasonably prevent the intentional use or disclosure of personally identifiable health information protected by HIPAA, and limit incidental uses or disclosures.
   3. Access to PHI is always limited to those who have a valid business or medical need for the information or otherwise have a legal right to know the information.

4. Unless being used to treat the affected individual, access to his or her PHI must, to the extent practicable, be limited to only that necessary to accomplish the intended purpose of the approved use, disclosure or request.
5. All access to physical areas/files and computer accounts/files that contain PHI should be limited to authorized personnel. This access will be revoked upon termination of employment, or when the individual no longer requires access to do his/her job.
6. Employees have the right to have access to their own PHI, may request an amendment to their own PHI, and may request an accounting regarding any disclosures that the Health Plan has made of their PHI to third parties.
7. The Health Plan may also use and disclose an individual's PHI without prior permission or authorization where the health information has been sufficiently "de-identified," so as to hide the identity of individual(s), or for other uses allowed by law.
8. Neither the Human Resources designee nor Fire Department personnel may share PHI except (a) as necessary for treatment, payment or health care operations; (b) as set forth in the attachments to this policy; (c) pursuant to a waiver of privacy rights via the HIPAA Authorization Form; or d) in accordance with a Business Associate Agreement.

H. Policy Violations

1. The following policy violations will result in disciplinary action, and may result in civil or criminal penalties:
2. Unauthorized use or disclosure of personally identifiable health information or PHI;
3. Attempting to make an unauthorized discovery of personally identifiable health information or PHI;
4. Failing to mitigate the unauthorized disclosure of personally identifiable health information or PHI;
5. Retaliating against or intimidating an individual who (a) exercises his or her privacy right(s); (b) files a complaint with the Department of Health and Human Services concerning HIPAA privacy violations; (c) participates in an investigation into a HIPAA privacy violation; or (d) participates in a HIPAA privacy compliance review;
6. Requiring an individual to waive his or her right to file a complaint of a HIPAA privacy violation as a condition for receiving treatment, payment, or enrollment in the Health Plan or eligibility for benefits;
7. Destroying privacy policies or procedures that are less than 6 years old;
8. Sharing personally identifiable health information or PHI with anyone who does not have the legal authority or the need to know the information to fulfill his or her job responsibilities;
9. Removing personally identifiable health information or PHI from the work area without authorization;
10. Failing to comply with the City's policies and procedures regarding the protection personally identifiable health information or PHI; and
11. Failing to report any unauthorized use or disclosure of personally identifiable health Information or PHI to the Privacy Officer.

I. Supervisory Responsibility

1. A supervisor who is asked by a subordinate or other employee about a claim under the City's Health Plan must not become involved in the issue unless the employee signs a HIPAA Authorization Form. Instead, the supervisor should refer the subordinate or other employee to Human Resources.