HEALTH INFORMATION PRIVACY

I. PURPOSE

To establish standards by which protected health information (PHI) is maintained and to provide you with a notice of the City's legal duties and privacy practices regarding your PHI.

II. SCOPE

This policy applies to employees, the administrators of the Plan and Departments listed in Resolution #012621-Q.

III. POLICY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes certain regulations that cover health plans and health care providers, including the City of Georgetown's (the "City") health plan ("Plan") and the Fire Department, which provides emergency health services. The City's Police Department, Information Technology Department, City Attorney's Office, Finance Department, City Manager's Office and City Secretary's Office are also included to the extent that each perform related covered functions. Because the City has many other functions besides providing a health plan, emergency medical services, and services performed by the Departments listed above, the City has designated itself as a hybrid entity. Therefore, no other departments except those listed above will be covered by the regulations. However, individual employees who are covered by the 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 rights.

IV. RESPONSIBILITIES

A. Privacy Officer

The Director of Human Resources & Organizational Development (Human Resources Director) or their designee is designated as the City's Privacy Officer for the Plan and the Departments or Offices listed above. Any questions about the

policies and procedures regarding this policy should be made to the Human Resources Director's attention. Also, any complaints about the violation of this policy or your rights as described in the Privacy Notice should be made to the Privacy Officer or complaints may be made to the Secretary of the Department of Health and Human Services. The Privacy Officer is responsible for the following:

1. Providing the HIPAA Privacy Notice to all Plan Participants, and maintaining acknowledgement of receipt of such notice;

2. Posting the attached HIPAA Privacy Notice, and all appropriate updates in a prominent place;

3. Posting the attached HIPAA Privacy Notice, and all appropriate updates on the City's web page;

4. Processing all complaints and documenting same, as well as the dispositions thereof;

5. Maintaining documentation of all complaints regarding privacy or other HIPAA violations for at least 6 years;

6. Fulfilling statutory responsibilities as the Plan's Privacy Officer, including overall responsibility for the Plan's compliance with HIPAA, its related regulations and the Plan's privacy and security policies;

7. Ensuring that all of the Plan employees who have access to Protected Health Information ("PHI") by virtue of their job duties are periodically identified;

8. Selecting and ensuring implementation of an initial and ongoing training program and then subsequent "new hire" training for all identified employees;

9. Ensuring that Business Associate Agreements are signed with any third parties to which the Plan gives PHI, and be the custodian for all Business Associate Agreements;

10. Monitoring compliance with the Plan's privacy and security policies including review to ensure that: (a) employees are given a HIPAA Privacy Notice and sign an Acknowledgement of Receipt of the HIPAA Privacy Notice ; (b) when PHI is used or disclosed to third parties, it is received a signed Authorization to Use and Disclose Health Information from the affected participant and that the disclosing employee complies with the accounting of disclosure procedures and placed a notation to the affected

participant's file; and (c) 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;

11. Serving as a resource for the Plan's employees or participants with questions about privacy standards and practices and/or patients' rights;

12. Serving as the conduit for providing any documentation required when any participant asserts rights under HIPAA (e.g., an accounting of all disclosures of PHI);

13. Monitoring legal and regulatory changes and suggest any needed policy and/or procedural changes;

14. Mitigate, to the extent practicable, any harmful effect that was caused by use or disclosure of PHI.

B. Covered Entity

1. Occasionally, an employee may contact the Human Resources Department concerning a claim for health care expenses. The Privacy Officer shall diligently protect the privacy of personally identifiable health information, unless the affected employee has waived his or her right of privacy under HIPAA. The above referenced Departments shall have in place appropriate administrative, technical, and physical safeguards to protect the privacy of personally identifiable health information. Those safeguards must reasonably prevent the intentional use or disclosure of any personally identifiable health information protected by HIPAA, and limit incidental uses or disclosures;

2. 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;

3. Unless being used to treat the affected individual, access to his or her PHI must, to the extent possible, be limited to only that necessary to accomplish the intended purpose of the approved use, disclosure or request;

4. All access to physical areas/files and or 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;

5. Employees have the right to access their own PHI, may request an amendment to their own PHI, and may request an accounting regarding any disclosures that have been made of their PHI to third parties;

6. The Plan or Departments listed above 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 as allowed by law;

7. In rendering emergency medical services, the Fire Department shall diligently protect the privacy of personally identifiable health information, unless the affected person has an Authorization to Use and Disclose Health Information. The notice is not required: (a) in cases of emergency; (b) where failure to use or disclose the PHI would compromise patient care; or (c) when otherwise specifically permitted or required by law;

8. Neither the Human Resources Department nor the Departments listed above may share personally identifiable health information except (a) as necessary for treatment or health care operations; (b) as set forth in the attachments to this policy; (c) pursuant to a waiver of privacy rights (Authorization to Use and Disclose Health Information); or (d) in accordance with a business associate agreement.

C. Supervisor

A supervisor who is asked by a subordinate or other employee about a claim under the City's Plan must not become involved in the issue. Instead, the supervisor shall refer the subordinate or other employee to the Human Resources Department Benefits Division.

V. PROCEDURE

A. Policy Violations

The following violations will result in disciplinary action, and may result in civil or criminal penalties:

1. Unauthorized use or disclosure of personally identifiable health information or PHI;

2. Attempting to make an unauthorized discovery of personally identifiable information or PHI;

3. Failing to mitigate the unauthorized disclosure of personally identifiable health information or PHI;

4. 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 an HIPAA privacy compliance review;

5. 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 Plan or eligibility benefits;

6. Destroying privacy policies or procedures that are less than 6 years old;

7. Sharing personally identifiable health information of PHI with anyone who does not have legal authority or the need to know the information to fulfill his or her job responsibilities;

8. Removing personally identifiable health information or PHI from the work area without authorization;

9. Failing to comply with the City's policies and procedures regarding the protection of personally identifiable health information or PHI; and

10. Failing to report any unauthorized use or disclosure of personally identifiable health information or PHI to the Privacy Officer.

B. Sanctions for Violations

Any person that violates this policy will be subject to sanctions, except that such sanctions will not apply to with respect to actions that are covered by and that meet the conditions of 45 C.F.R. §§ 164.502(j) or 164.530(g)(2).

C. HIPAA's Effect on Other Health Care Information

Neither HIPAA nor this policy affect personally identifiable health care information required for life insurance, disability insurance, workers' compensation, or employment records (such as records of absences or tardiness for health reasons, Family Medical Leave Act Records, or records reflecting a need for a reasonable accommodation pursuant to the Americans with Disabilities Act) kept by the City in its capacity as an employer.