City of Burleson

Summary

of the City's Privacy Policy and Procedures for the Employee Benefit Plan

May 30, 2014

I. Purpose

The purpose of this summary of the City's HIPAA Privacy Policy and Procedures ("Policy") is to ensure that employees of the City of Burleson who administer or perform functions on behalf of the City's Employee Benefit Plan (the "City Health Plans" or the "Plan") comply with regulations related to (1) the federal HIPAA Privacy Standards, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and (2) the Texas Medical Records Privacy Act as it relates to the City Health Plans. This summary document is adopted to provide employees notice of the full policy. A complete copy of the City's Policy can be obtained from the Human Resources Department.

II. Definitions

Any term not defined within this summary document is defined fully in Article II. of the Policy on pages 1 – 8.

III. Applicability

City's Medical Privacy Obligations as a Health Plan

Because the City offers employer sponsored group health benefit plans that are self-insured, and there are over fifty (50) participants, the City's Health Plans must comply with HIPAA. This is true even though the City contracts with a third party administrator for administrative services. The Policy applies to the City's Health Plans. (Please note, the Policy only applies to the City's Health Plans. Any responsibilities the City has as a Health Care Provider because the Fire Services Department provides ambulatory services and its first responders provide medical care are outlined in a separate document. [*See* the City of Burleson adopted policy entitled *City of Burleson HIPAA Security Policies and Procedures for the Fire Department* for the requirements applicable to the City as a Health Care Provider.])

City as a Plan Sponsor

Because the City sponsors the City's Health Plans for the benefit of its employees and their eligible dependents and beneficiaries, the City is considered the Plan Sponsor. However, the Plan Sponsor is a legally separate entity from the Health Plans. Because of this legal separation, the Privacy Standards and the Policy prohibit the City's Health Plans from sharing PHI with the Plan Sponsor, except as required or permitted by the HIPAA Privacy Standards. These requirements are addressed more fully in the Policy on page 64 in Article V, Part C., "Separation of the Plan from the Plan Sponsor."

City's Medical Privacy Obligations as Employer

Under HIPAA, the City is not a covered entity if it simply holds medical information about a City employee in its role as an employer. However, the City must still comply with the Texas Medical Records Privacy Act regarding information held in its capacity as employer. These requirements are outlined on page 9 of the Policy.

City's Health Plans as an Organized Health Care Arrangement

See page 10 of the Policy for an explanation of Health Care Arrangement.

IV. HIPAA Requirements

A health plan is required under the Privacy Standards to develop procedures for handling the privacy of individually identifiable health information. The City's Policy has been adopted in compliance with the Privacy Standards.

Compliance with the Privacy Standards and the Policy is Required

The employees of the Human Resources Department who are responsible for administering the City's Health Plans or who perform functions on behalf of the City's Health Plans (the "Plan") must comply with all policies and regulations mandated by federal and state governments regarding the confidentiality, integrity and availability of a participant's PHI, including HIPAA, HITECH and the Texas Medical Records Privacy Act. All Department employees must adhere to the policies and practices outlined on page 11 of the Policy.

V. HIPAA Privacy Fundamentals

To comply with the Privacy Standards, the City should do three things: (1) only use and disclose PHI as permitted or required by the Privacy Standards; (2) be aware of and respect individual rights under the Privacy Standards; and (3) comply with administrative responsibilities under the Privacy Standards.

A. General Rule for Use or Disclosure of PHI

The Plan may not use or disclose a participant's PHI without authorization from the participant unless the use or disclosure is: (1) to the individual who is the subject of the protected information; (2) for treatment, payment or health care operations as permitted under the Privacy Standards; (3) to evaluate health plan performance; (4) for underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits; (5) to conduct or arrange for a medical review, legal services, auditing functions, including fraud and abuse detection and compliance programs; (6) for business planning and development; (7) for business management and general administrative activities, and fundraising for the benefit of the City's Health Plans (provided an authorization of use or disclosure of the PHI for fundraising purposes is obtained from the individual).

Additionally, see *Business Associates* on page 67 of the Policy, Article V, Part C., and "Administrative Requirements" of the Policy for more detail regarding other entities obligations as it relates to their use or disclosure on behalf of the City.

1. Minimum Necessary Standard for the Use or Disclosure of PHI

The Plan must limit the use or disclosure of PHI to the minimum necessary amount of PHI needed to carry out the purposes for or use of the information disclosed. The Plan limits the use or disclosure of PHI, including the request of PHI from other entities, to the extent practicable to a limited data set; if more information is needed, the use, disclosure and request is limited to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with applicable laws. See pages 14 – 19 of the Policy for additional information.

2. Participant Authorization to Use or Disclose PHI

The Plan will release PHI pursuant to a valid authorization. The Policy on pages 19 – 22 provides a procedure for obtaining participant authorization for the use or disclosure of PHI when required by law.

3. Permitted Use or Disclosure for Treatment, Payment or Health Care Operations

The Plan may use or disclose PHI for treatment, payment, or health care operations. For example:

- The Plan may disclose PHI to a health care provider to help ensure appropriate treatment.
- The Plan may disclose PHI to health care provider to facilitate payment to the health care provider
- The Plan may disclose PHI to another covered entity for certain health care operations such as disclosures for:
    - Conducting quality assessment and improvement activities;
    - Patient safety activities; and population based activities relating to improving health or reducing health care costs.
    - Health care fraud and abuse detection. [45 C.F.R. § 164.506(c)(4)].

See pages 23 – 24 of the Policy for additional information regarding disclosures for treatment, payment, or health care operations.

4. Permitted Disclosure to Personal Representative(s)

Adult or Emancipated Minor

The Plan may disclose information to a personal representative of an individual participant if that person is authorized by law to act on behalf of the participant in making decisions related to health care for the participant. See page 24 of the Policy for additional information.

Minors

The Plan must treat a parent, guardian or other individual who is acting *in loco parentis* who has the authority to act on behalf of a minor with respect to health consideration as a personal representative except in certain instances outlined on page 25 of the Policy.

5. Permitted Disclosure regarding Deceased Individual(s)

Plan employees must comply with the Privacy Standards with respect to the PHI of a deceased individual. If, under applicable law, an executor, administrator or other individual has authority to act on behalf of a deceased participant or of the participant's estate, a Plan employee will treat such individual as a personal representative with respect to PHI relevant to such personal representation.

Plan employees may also disclose PHI to funeral directors, as necessary, to carry out their duties with respect to the decedent. Such information may also be disclosed to a funeral director prior

to or in reasonable anticipation of a participant's death if it is necessary for the funeral director to carry out his or her duties.

6. Permitted Disclosure to Business Associate(s)

The Plan may disclose PHI to a Business Associate and allow the Business Associate to create or receive PHI on its behalf only if the City has an agreement with that Business Associate. The Policy contains more information regarding permitted disclosures to a Business Associate on pages 25 – 26.

7. Other Permitted Disclosures

Disclosures by Whistleblowers

A Plan employee may disclose PHI, if that employee believes in good faith that the City engaged in conduct that is unlawful, or otherwise violates professional standards, or the care, services or conditions provided by the City potentially endangers one or more patients, participants, employees or the public. To be lawful, such a disclosure must be to specific entities or individuals. See page 26 of the Policy for more information.

Disclosures by Workforce Crime Victims

A Plan employee who is the victim of a criminal act may disclose PHI to a law enforcement official, provided that the PHI disclosed is about the suspect of the criminal act and the PHI disclosed is limited to disclosures to law enforcement for the use of identifying or locating a suspect, fugitive, material witness or missing person. See page 27 of the Policy for more detail.

8. Use or Disclosure for Which Authorization is Required

The following uses or disclosures require an authorization before the use or disclosure may be carried out. See pages 27 through 31 of the Policy for more details regarding each use or disclosure:

Authorization for Use or Disclosure of Psychotherapy Notes

Psychotherapy notes are notes recorded by a health care provider who is a mental health professional providing, documenting or analyzing the contents of a conversation during a counseling session, or a group, joint or family counseling session that is separate from the rest of the individual's medical records.

Authorization for Marketing

The Plan must obtain a participant's or employee's clear and unambiguous authorization for any use or disclosure of PHI for marketing, except in certain instances outlined on pages 28 – 29 of the Policy.

Authorization for Re-identification

The Plan may not re-identify or attempt to re-identify a participant who is the subject of any PHI without obtaining the participant's consent or authorization.

Authorization for Sale of PHI

The Plan may not allow any other person to access the PHI or license or lease the PHI of a participant or employee in exchange for direct or indirect remuneration unless certain criteria, outlined on page 29 of the Policy are met.

Authorization for Fundraising

The Plan may use, or disclose to a business associate, the PHI outlined on page 30 of the Policy for the purpose of raising funds for the City Health Plans' benefit without an authorization. However, the Plan may not use or disclose PHI for fundraising purposes unless the Plan includes a statement in its notice of privacy practices that it intends to contact the participant to raise funds and provides the individual the right to opt-out of receiving such communications. The Plan may not make fundraising communications to a participant where such participant has elected not to receive such communications.

Electronic Disclosure of PHI

The Plan must provide notice to a participant for whom it creates or receives PHI if the individual's PHI is subject to electronic disclosure. See page 31 of the Policy for more information regarding electronic disclosure of PHI.

9. Use or Disclosure with Opportunity to Agree or Object

Unless written consent is required by law, the Plan may use or disclose PHI under the circumstances listed below and detailed more fully on page 32 of the Policy, provided that the participant is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit the use or disclosure.

- Use or Disclosures for Involvement in the Participant's Care and Notification Purposes
- Uses or Disclosures when the Participant is Present
- Use or Disclosures for Disaster Relief

10. Uses or Disclosures for Which No Authorization or Opportunity to Object is Required

In situations where an authorization or an opportunity to object is not required, the Plan may use or disclose PHI without obtaining written authorization of the participant or providing the participant with the opportunity to agree or object. See pages 32 – 40 of the Policy. The following situations do not require authorization or opportunity to object:

Uses or Disclosures Required by Law

To the extent use or disclosure is required by law, the Plan may disclose PHI. A disclosure is required by law if there is a mandate that compels the Plan, to make a use or disclosure of PHI that is enforceable in court. See page 33 of the Policy.

Disclosures for Public Health Activities

The Plan may disclose PHI for public health activities to certain health authorities in limited circumstances. See pages 33 – 34.

Disclosures for Health Oversight Activities

The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law. See pages 34 – 35 of the Policy.

Disclosures for Judicial and Administrative Proceedings

The Plan may disclose PHI in the course of any judicial or administrative proceeding as required by court order or if the Plan receives satisfactory assurances. See pages 35 – 36 of the Policy.

Disclosures for Law Enforcement Purposes and Pursuant to Process and as Otherwise Required by Law

The Plan may disclose PHI as required by law, including laws that require the reporting of certain types of wounds or other physical injuries, or in compliance with, and as limited by, the relevant requirements of certain legal process as outlined on page 36 of the Policy.

Permitted Disclosures for Identification and Location

The Plan may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that certain conditions outlined on pages 36 – 37 of the Policy are met.

Permitted Disclosures of Victims of a Crime

A Plan may disclose PHI in response to a law enforcement official's request for information about a participant who is, or is suspected to be, a victim of a crime if the participant agrees to the disclosure. If a Plan is unable to obtain an agreement from a participant because of incapacity or other emergency circumstances, the Plan may disclose PHI to law enforcement if certain conditions, outlined on Page 37 of the Policy, are met.

Permitted Disclosures Regarding Decedents

The Plan may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased individual, determining a cause of death, or other duties as authorized by law.

Permitted Disclosures Regarding Crime on Premises

The Plan may disclose to a law enforcement official PHI that the Plan believes, in good faith, constitutes evidence of criminal conduct that occurred on the premises of the Plan.

Permitted Uses or Disclosures for Organ, Eye or Tissue Donation

The Plan may use or disclose PHI to an organ procurement organization.

Permitted Uses or Disclosures to Avert a Serious Threat to Health or Safety

The Plan may use or disclose PHI if the Plan, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public; is necessary to law enforcement to identify or apprehend an individual admitting participation in a violent crime; or because the individual has escaped from a correctional institution or from lawful custody. See pages 38 - 39 of the Policy for more information.

Uses or Disclosures for Specialized Government Functions

The Plan may use and disclose PHI of participants for certain specialized governmental functions outlined on pages 39 – 40 of the Policy.

Uses or Disclosures for Underwriting and Related Purposes

The Plan may use or disclose PHI for purposes of activities related to the creation, renewal, and replacement of contracted health insurance. See page 40 of the Policy.

11. Verification Requirements for Permitted Disclosures

The Plan shall comply with authority and identity verification requirements prior to making any disclosure of PHI. The verification requirements are more fully described on pages 40 – 42 of the Policy.

B. Individual Rights

There are seven individual rights under the Privacy Standards of which Plan personnel must be aware. These are:

- Right to receive Notice of Privacy Practice;
- Right to an Accounting of Disclosures of PHI;
- Right to Request Restrictions on Use or Disclosure of PHI;
- Right to Request Correction or Amendment of PHI;
- Right to Access PHI;
- Right to Request Confidential Communications regarding PHI; and
- Right to File a Complaint regarding Use or Disclosure of PHI.

All Plan personnel must respect these individual rights under the Privacy Standards.

1. Notice of Privacy Practices

The Plan is required to provide participants with a Notice of Privacy Practices ("NPP") that is written in plain language. See pages 43 – 44 of the Policy for more details regarding the requirements for a NPP.

2. Participant Right to an Accounting of Disclosures of PHI

The Plan shall maintain an accounting of all uses or disclosures of all PHI maintained by the Plan for a period of six (6) years. A participant may request an accounting for a period of up to six (6) years from the date of the request or less. See pages 45 – 48 of the Policy for details on how to request an accounting and exceptions to the right to receive an accounting.

3. Participant Right to Request Restriction on Use or Disclosure of PHI

A participant has the right to request a restriction of the use or disclosure of the Participant's PHI. The Policy provides a process for handling requests by participants or their legally authorized representatives to request a restriction of the use or disclosure of the participant's PHI consistent with federal law. See pages 48 – 50 of the Policy for that process.

4. Participant Right to Request Correction or Amendment of PHI

A participant has the right to request that the Plan amend his or her PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. The Policy provides a process for handling requests by participants to request a correction or amendment of the participant's PHI maintained in a designated record set by the Plan consistent with federal law on pages 50 – 55.

5. Participant Right to Access Their PHI

A participant has a right of access to inspect and obtain a copy of his or her PHI in a designated record set for as long as the PHI is maintained in the designated record, subject to certain exceptions. The Policy provides a process for handling requests by a participant or his or her legally authorized representative to access and/or copy the participant's PHI that is consistent with federal and state law on pages 55 - 61.

6. Participant Right to Request Confidential Communications

A participant has the right to request that the Plan communicate PHI to him or her via specified confidential means. The Policy provides a process for a participant to request confidential communications regarding his or her PHI that is consistent with federal and state law on pages 61 – 62.

7. Participant Right to File a Complaint Regarding Use or Disclosure of PHI

A participant has the right to file a complaint with the Plan, state government or the federal government if the person believes that the Plan is not complying with the HIPAA Privacy and Security Standards. The Policy provides a process for a participant to file a complaint regarding the Plan's use or disclosure of his or her PHI that is consistent with federal and state law on pages 62 – 64.

C. Administrative Requirements

1. Separation of the Plan from the Plan Sponsor

The Privacy Standards require the Plan to restrict the disclosure of PHI to the Plan Sponsor. The Plan and the Plan Sponsor must abide by the procedures outlined on pages 65 – 67 of the Policy to make sure that the disclosure is properly restricted.

2. Business Associates

The Plan may disclose PHI to its Business Associates, and may allow a Business Associate to create or receive PHI on its behalf, if and only if the Plan has an agreement with the Business Associate. The Policy provides procedures to ensure that all contracts and agreements between the Plan and its Business Associates comply with the requirements of the Privacy Standards on pages 67 – 70.

3. Privacy Officer

The Plan must designate a Privacy Officer. All requests for access, accounting of disclosures, restrictions, confidential communications or an amendment to participant records that are received by employees shall be referred to the Privacy Officer.

As of the effective date of this Policy, the Plan's Privacy Officer is:

Director of Human Resources (817) 426-9644

The Privacy Officer will be responsible for monitoring employee and Plan compliance with all state and federal privacy standards. Should a complaint or accusation arise against an employee or the Plan regarding compliance with the Policy or the Privacy standards, the Privacy Officer is designated as the Complaint Officer, and will investigate the complaint and follow Plan procedures regarding appropriate disciplinary action if the investigation supports the complaint. If an employee has been disciplined due to non-compliance with this Policy, the Privacy Officer shall ensure that the provision of the Policy violated and the sanction imposed is documented. In the event a complaint involves the Privacy Officer, the complaint shall be referred to the City Attorney's Office.

4. Workforce Training

The Plan must train all members of its work force who are designated to act on behalf of the City's Health Plans, or who have access to PHI as necessary and appropriate for personnel to carry out their functions. All Plan employees must attend training and periodic updates on the HIPAA Privacy and Security Standards, the Texas Medical Records Privacy Act and this Policy. See pages 71 – 73 of the Policy.

5. Sanctions

The Plan will apply appropriate sanctions against an employee who fails to comply with the Policy; all sanctions must be documented. The Policy provides a guideline for issuing discipline to correct employee conduct that violates the Privacy Standards or the Policy on page 73. Discipline will be imposed per the City's Employee Handbook.

6. Mitigation

The Plan protects the privacy and confidentiality of PHI and will take reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to the Plan of a use or disclosure of PHI in violation of the Privacy Standards or the Policy. "Reasonable steps" include contacting the individual who is the subject of the PHI and the appropriate authorities to inform them of the violation, and could include consulting with the individual regarding steps he or she believes are necessary to prevent further harm. A reasonable step would also include contacting the recipient of the improper disclosure and advising them not to use or further disclose the information. See pages 73 - 74 of the Policy for additional mitigation requirements.

7. Breach of Unsecured Protected Health Information

HIPAA Privacy and Security regulations require that individuals be notified when a covered entity knows, or should have known, of a breach of unsecured PHI that poses a significant risk of harm to the individuals has occurred. In the event of a breach of PHI, the Privacy Officer will conduct a risk assessment. See pages 74 – 75 of the Policy for breach notification and risk assessment requirements.

8. Intimidating or Retaliatory Acts Prohibited

The Plan may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against: (1) any individual for exercising any right under the Privacy Standards; or (2) any

participant, or other person, for filing a complaint with the Secretary of HHS or the Office of the Attorney General; testifying, assisting or participating in an investigation, compliance review, proceeding or hearing; or opposing any unlawful act or practice.

9. Waiver of Rights Prohibited

The Plan may not require individuals to waive their rights to make complaints to the Secretary of Health and Human Services or the Office of the Attorney General as a condition of the provision of treatment, payment or enrollment in a health plan or eligibility for benefits.

10. Changes to Policy and Procedures

The Plan must implement the policy and procedures with respect to PHI that are necessary to comply with the Privacy Standards. See pages 75 – 77 of the Policy.

11. Documentation and Retention Requirements

The Plan must retain all documents related to the Policy for a period of six (6) years from the date it was created or it was in effect, whichever is later. See page 77 of the Policy.

VI. Enforcement

A person who knowingly obtains or discloses PHI in violation of the Privacy Rule may face criminal and/or civil penalties as outlined on pages 77 – 79 of the Policy. The U.S. Department of Justice is responsible for criminal prosecutions under the Privacy Rule. The U.S. Department of Health and Human Services, Office of Civil Rights is responsible for civil enforcement and may impose a civil penalty for a failure to comply with the Privacy Standards.

In addition, the Texas Attorney General may institute an action for injunctive relief to restrain a violation of the Texas Medical Records Privacy Act. In addition to injunctive relief, the Texas Attorney General may institute an action for civil penalties against a covered entity for a violation of the Texas Medical Records Privacy Act.