Privacy Policy

1.0 POLICY STATEMENT: The privacy of our employees is important to the City. The City understands the importance employee's place on the protection of personal and medical information in the City's health benefits plans. As a covered employee there may be inquiries about surgical or medical procedures to determine benefit eligibility, benefit payments and other business transactions associated with the City's health benefits plans.

2.0 PROCEDURES: The City's Privacy Policy will explain what information is collected, how that information is protected; and the choices you have about how that information is used. Please review the City's Privacy Policy in order to understand the City's commitment to you and your privacy, and how you can participate in that commitment. The following sections make up our Privacy Policy. We hope that by reading them, you will have a clear idea of how we manage information we provide our business associates and our employees.

2.1 *Legal Context of HIPPA* - HIPAA is the Health Insurance Portability and Accountability Act of 1996. The act includes specific rules regarding administrative simplification, which require: 1) More efficient healthcare delivery through standardized electronic data interchange, and 2) Increased and standardized protection of the confidentiality and security of health data.

2.2 *How the Law is Applied* - All health plans are covered entities under the HIPAA regulations and must comply with the privacy and security regulations of HIPAA. The City's health benefits plan is a covered entity and sets forth this policy and procedure to comply with HIPAA. The City will accomplish compliance with HIPAA through the Department of Human Resources staff. The Director of Human Resources will serve as the Compliance Coordinator and the Privacy Officer to ensure initial compliance and continuous maintenance of the HIPAA program as the law changes.

2.3 *Glossary of Terms* - HIPAA has its own language; special terms that you need to understand in order to accomplish compliance efforts. This glossary provides these specific definitions. Please note that these are working definitions (and not the exact legal definitions) that are easier to read and understand.

a. Business Associate - A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

b. Compliance Date – The date by which a covered entity must comply with a standard, implementation specification, requirement, or modification. Usually 24 months after the effective date of a standard.

c. Chain of Trust - A term used in the HIPAA Security regulations for a pattern of agreements that extend protection of health care data by requiring that each covered entity that shares health care data with another entity require that that entity provide protections comparable to those provided by the covered entity, and that that entity, in turn, require that any other entities with which it shares the data satisfy the same requirements.

d. Code Set – Any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions.

e. *Covered Entity* – (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

f. *Electronic Data Interchange (EDI)* – Electronic exchange of formatted data using defined and accepted industry standards.

g. *Effective Date* – The date that a final rule is effective, usually 60 days after it is published in the Federal Register.

h. *FAQ(s)* – Frequently Asked Question(s).

i. *Group Health Plan* – An employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002 (1)), including insured and self-insured plans, so long as the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise. To qualify as a covered entity, a group health plan must have either 50 or more participants or is administered by someone other than the employer that established and maintains the plan.

j. *HHS* – The Department of Health and Human Services, the administrative body responsible for determining the HIPAA regulations and ensuring their enforcement.

k. *Health Care* – Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to: (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

l. *Health Care Clearinghouse* – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from

another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

m. *Health Care Provider* – A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395X(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

n. *Health Information* – Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) 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.

o. *Health Care Operations* – The use of PHI is restricted by the privacy rule, except for treatment, payment and Health Care Operation activities. Health care operations, as defined by the statute, include: (1) conducting quality assessment and improvement activities (2) accrediting/licensing of health care professionals (3) evaluating health care professional performance (4) training future health care professionals (5) activities relating to the renewal of a contract for insurance (6) conducting or arranging for medical review and auditing services (7) compiling and analyzing information for use in a civil or criminal legal proceeding.

p. *Health Plan* – An individual or group plan that provides, or pays the cost of, medical care. This includes all group health plans that provide or pay for any type of medical care.

q. *Implementation Specification* – Specific requirements or instructions for implementing a standard.

r. *Incidental Use & Disclosure* – Unintended uses and disclosures of PHI that occur as a byproduct of a use or disclosure otherwise permitted under the Privacy Rule. An incidental use or disclosure is permissible only to the extent that the covered entity has applied reasonable safeguards as required by the regulations and has implemented the minimum necessary standard, where applicable, as required by the regulations.

s. *Individually Identifiable Data* – Data that can be readily associated with a specific individual. Examples would be a name, a personal identifier, or a full street address. Includes data that alone could not identify an individual, could collectively identify an individual.

t. *Limited Data Set and Data Use Agreement* – A set of limited data which has been de-identified of all of the facially identifying information and a few other direct identifiers. For a covered entity to disclose a limited data

set to a recipient they must first obtain a "data use agreement" from the recipient of the data. The data use agreement spells out the terms under which the recipient agrees to use or receive the data. It also includes similar language to the Business Associate agreement to ensure that the recipient uses appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the HIPAA regulations.

u. *Marketing Communications* – Marketing is defined as follows: To make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service. There are three categories of communications that are excluded from the definition of marketing (which means that the covered entity is not engaged in marketing when it communicates to individuals about: (1) The participating providers and health plans in a network, the services offered by a provider, or the benefits covered by a health plan; (2) the individual's treatment; or (3) case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual. For example, supplying a list of participating providers to members does not constitute marketing under HIPAA.

v. *"Minimum Necessary" Rule or Minimum Scope of Disclosure* – The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.

w. *Office for Civil Rights (OCR)* – The entity within the Department of Health and Human Services (HHS) responsible for enforcing the HIPAA privacy rules.

x. *Payer* – An entity that assumes the risk of paying for medical treatments. This can be an uninsured patient, a self-insured employer, a health plan, or an HMO.

y. *Protected Health Information (PHI)* – Individually identifiable health information that is transmitted or maintained in any form or medium, including electronic, written, oral or other.

z. *Standard* – A rule, condition, or requirement: (1) Describing the following information for products, systems, services or practices; (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of individually identifiable health information.

aa. *Standard Setting Organization (SSO)* – An organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, these regulations.

bb. *Trading Partner Agreement* – An agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or

part of a larger agreement, between each party to the agreement. For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction. See Chain of Trust.

cc. *Transaction* – The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Other transactions that the Secretary may prescribe by regulation.

dd. *Workforce* – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

2.4 *HIPPA Privacy Officer* - The Director of Human Resources serves as the City of Johnson City's Privacy Officer. In this capacity, the Privacy Officer oversees all ongoing development, implementation, maintenance of, and adherence to the City's policies and procedures covering the privacy of and access to protected health information in compliance with federal and state laws and the City of Johnson City's information privacy practices.

2.5 *Privacy Rule* - The Privacy Policy of the City of Johnson City follows national standards to protect employee's medical records and other personal health information.

2.6 *Notice of Privacy Practices* - As required by HIPAA, the City of Johnson City will explain the requirements to maintain the privacy of employee health information and how the City may use and disclose protected health information. The City may use and disclose your medical records only for each of the following purposes:

a. Treatment – Means providing, coordinating, or managing health care and related services by one or more health care providers. An example of this would include case management.

b. Payment – Means such activities as obtaining reimbursement for services, confirming coverage, billing or collection activities, and utilization review. An example of this would be adjudicating a claim and reimbursing a provider for an office visit.

c. Health Care Operations – Include the business aspects of managing the health care plan, such as conducting quality assessment and improvement activities, auditing functions, cost management analysis, and customer service. An example would be an internal quality assessment review.

2.7 *Access to Notice of Privacy Practices* - A Notice of Privacy Practices is available for review in the Department of Human Resources. The Human Resources Department will:

a. Adopt and maintain on file the current Notice of Privacy Practices
b. Will make available upon request paper copies of our current Notice of Privacy Practices
c. Modify the Notice of Privacy Practices as needed with approval of the City Manager;
d. Will retain all versions for not less than six (6) years following the last use of the version; and
e. Provide copies of the Notice of Privacy Practices to current employees and provide copies of the Privacy Policy to new employees.

2.8 *Records Access* - All staff of the Privacy Office will accommodate an employee's written request to see a copy of his or her medical records as they relate to the City's health benefits plan. The request must be in writing and signed and dated by the covered employee or their personal representative. If the request is to see the record, the employee may have immediate access within the Human Resources office if that record is on file. Since the Health Plan Administrator maintains those records as part of its administrative services agreement, the City will assist in contacting the Health Plan Administrator to get access to specific records. Any records that are requested that the Human Resources Department can provide will be done with the supervision of the Privacy Officer to ensure the record remains intact and unaltered. The City may deny such request only if the life of the covered person would be endangered by such disclosure.

2.9 *Records Amendment* - The staff of the Human Resources Department will accommodate a covered employee's written request to amend his or her medical record. The request must be in writing and signed and dated by the individual or their legal guardian. Since the majority of the medical records are on file with the Health Plan Administrator, Human Resources will assist the employee in obtaining those records for amendment. The City will follow procedures to ensure that the covered employee has access to amend their medical records on file with the health plans administrator.

2.10 *Non-Routine Disclosures* - The Human Resources Department will assist with a covered employee's written request of the plan administrator in obtaining a history of non-routine disclosures of their protected health information. If an authorization is received the Human Resources Department will assist the covered

2.11 employee in obtaining the disclosures. The request must be in writing and signed and dated by the covered employee's legal guardian. Every attempt will be made by the Human Resources Department to have the request satisfied by the plan administrator within 30 days. The Privacy Officer is responsible for ensuring that all requests to the plan administrator are fulfilled in a timely manner.

2.12 *History of Non-Routine Disclosures Report* - The Human Resources Department will keep a record of all requests for non-routine disclosures made in writing in Human Resources. Since the Health Plan Administrator keeps records of non-routine disclosures, the Human resources Department will assist by maintaining a record of request made to the Human Resources Department.

2.13 *Privacy Grievance Policy and Procedure* - The Privacy Officer for the City of Johnson City will work with the health benefits plan administrator to investigate all reported incidents of alleged violation of health information privacy, regardless of the source and severity. The Privacy Officer will maintain a Privacy Incident file, and will provide summary reports to management on the status of each open file regarding alleged health information privacy violations. The Privacy Incident file will contain:

a. Written documentation of the alleged violation by the covered individual or other reporting entity.
b. A plan of action documenting the planned course of the investigation.
c. Complete documentation of the investigation, including transcripts of all interviews.
d. Documentation of all correspondence regarding the alleged violation.
e. Documentation of the decision regarding the alleged violation and documentation as to the resolution of the alleged violation.
f. Documentation of all reported incidents will be maintained for the time required by law (six years following last action).

2.14 In the event of an employee files grievance regarding a violation of the health information privacy, the order of escalation shall be: 1) The Privacy Officer, and 2) Fiduciary or officers of the health plan (third party administrator).

2.15 Procedure for Filing Grievance - If an employee feels their data privacy has been compromised:

a. The individual should discuss the situation with the Privacy Officer.
b. The Privacy Officer will log the complaint in the Incident File and will determine if the complaint can be resolved in an informal manner. Documentation of the informal resolution will be provided.
c. If the complaint cannot be resolved informally the affected individual will provide a written statement of the complaint.

A written proposal of resolution will be developed and may include:

d. An apology.
e. A description of a process change that will prevent reoccurrence.
f. An invitation to discuss the situation further.
g. Addresses of appropriate professional, state and federal offices to which the complaint may be escalated.
h. Review the complaint and proposed resolution with City Senior Management.
i. File the written complaint and the proposed resolution in the Privacy Incident File.
j. If a procedure change is warranted, a modification process will be documented to reflect the change and the Privacy Officer will communicate the change to all affected staff.
k. There will be a follow up with the person filing the grievance until they are satisfied or the problem has been escalated to the next level for review

2.16 *Restriction of Records* - If a covered employee asks for a restriction of protected health information, the Privacy Officer and the Health Plan Administrator will:

a. Accommodate the covered persons written request to restrict some or all of the protected health information in his or her medical record.
b. The request must be in writing and signed and dated by the covered person.
c. A decision regarding allowing the restriction shall be made as soon as reasonably possible.
d. If a decision to deny the restriction is made, a written explanation shall be returned to the requestor by U.S. mail.
e. If the restriction is allowed, a notification will be made to the file immediately.
f. If the restriction is allowed the protected health information will not be disclosed except in emergency situations or to public health, government or law enforcement officials with the proper documentation.
g. If the requestor cancels this restriction, a notation will be made and entered into the medical record.

2.17 *Health Care Information Privacy* - Employees that have proper access to protected health information to perform the duties of their positions with the City must not discuss or share that protected data outside the office or with other covered persons. Employees must not leave employee's records unattended in public areas of the office. Employees may only access protected health information for which they have a legitimate, assigned business need. Employees may not remove any files or copies of files from the office without proper authorization. Records waiting to be updated or any uncompleted work involving protected health data must be locked in a file cabinet at the close of each business day.

2.18 *Information Requests* - The City will only respond to requests for information in writing. We will only respond to information requests as allowed by the regulations and when we have a properly completed and executed authorization form for the specific information, recipient and time period requested, or if the request can be satisfied thorough fully de-identified data. The appropriate documentation of all requests will be maintained and we will always provide only the minimum information necessary to satisfy the specific request. The City will follow protocols that have been established by HIPAA regulations regarding routine disclosures.

2.19 *Self-Initiated Uses and Disclosures* - The City will not initiate or allow disclosure of protected health information held by the health plan for:

a. Employment related decisions including, but not limited to hiring, firing, job selection and promotion decisions.
b. Use by non-health plan benefits, except as specifically allowed by law (i.e. worker's comp)

The City may initiate or allow disclosure of protected health information for:

c. Worker's compensation plan administration.
d. A health insurance carrier or underwriter for purposes of underwriting a new contract or renewal of an existing contract for insurance.

2.20 *Firewall Policy* - The City and its business associates will only use health plan data for health plan related decisions. Secure storage and computer access to records held by the health plan will be provided to minimize inappropriate access. Health plan data will not be used for employment related decisions or transferred to any non-health plan without prior written authorization by the covered individual.

a. Specific individuals and job classes have been designated who will have access to protected health information. As allowed and required by law, only those designated individuals shall have access to PHI without explicit authorization by a covered member. Training on the HIPAA law will be conducted for those individuals and a confidentiality agreement will be signed.

2.21 *Authorizations* - The Privacy Officer will always obtain properly signed and dated authorization forms for protected health information. A copy of the signed authorization will be kept in the covered member's file. The Privacy Officer will maintain authorization forms on file for six years after their expiration date or event.

2.22 *De-Identification* - As the plan sponsor, the City of Johnson City will assist the Health Plan Administrator in de-identifying all health data when in our

professional judgement, the de-identified data will satisfy the request that has been made. The City will take steps to ensure that all 18 requirements listed below have been properly removed and that any remaining identifying elements cannot be used to directly retrieve member data from any other available source:

a. Names
b. All geographic subdivisions smaller than a state, including street addresses, city, county, precinct, and zip codes
c. All elements of dates directly related to an individual including birth date, admission date, discharge date, date of death, and all ages and elements of dates indicating age
d. Telephone Numbers
e. Fax numbers
f. E-mail addresses
g. Social security numbers
h. Medical record numbers
i. Health plan beneficiary numbers
j. Account numbers
k. License numbers
l. Vehicle identifier and license plate numbers
m. Device identifiers and serial numbers
n. Web universal resource locators
o. Internet Protocol (IP) address numbers
p. Biometric identifiers, including finger and voice prints
q. Full face pholographic images and any comparable images
r. Any other unique identifying number, characteristic, or code

2.23 *Minimum Necessary Information Access* - To maintain the confidentiality of health data, the City will follow the minimum necessary information principle, which minimizes the amount of protected health information used and disclosed within the City organization and the number of persons who have access to this information. The City will take reasonable steps to limit the use or disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

2.22.1 Disclosures to or requests by a health care provider for treatment purposes
2.22.2 Disclosures to the individual who is the subject of the information
2.22.3 Uses or disclosures made pursuant to any valid authorization received by a health care provider
2.22.4 Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act transactions
2.22.5 Disclosures to the Department of Health and Human Services when disclosure of information is required for enforcement purposes
2.22.6 Uses or disclosures that are required by other laws

2.23 *Breach of Information Privacy* - The Privacy Officer is responsible for investigating all reported incidents of alleged violation of health information privacy, regardless of the source or severity. All documents related to alleged violation will be kept in an Incident File. If an employee becomes aware that health data privacy has been compromised:

2.23.1 Employee must immediately report the breach to the Privacy Officer.

2.23.2 The Privacy Officer will analyze the breach and decide what level of breach has occurred.

a. Very Serious – A large amount of data, or very sensitive data has been made public.

b. Serious - A large amount of data has potentially been exposed, but the likelihood of it being accessed is slim.

c. Important – Protected health information has been inappropriately released to a trusted business partner

d. Minor – Protected health information has been handled carelessly, but no exposure occurred.

2.23.3 Analyze the problem and decide level of culpability.

2.23.4 Log the breach in the Privacy Incident File and log the level of breach.

2.23.5 Develop a plan of action to remedy the breach and notify appropriate persons of the appropriate solution and consequences of the breach.

2.23.6 Record the action plan in the Incident File.

2.23.7 Conduct internal investigation to determine if policies and procedures need to be modified.

2.23.8 Document the progress and outcome of the investigation and place in the Incident File.

2.24 *Record Storage and Access* - Employee health information will be maintained and secured separately from all employee records and shall not be comingled with employment records of any kind. The City will also ensure that archived files will also be secured and reasonably safeguarded. Covered employees health information stored on computers will be password protected.

2.25 *Disposal of Protected Health Information* - The City will ensure that handwritten notes such as paper phone messages containing protected health information will be shredded as soon as they are no longer needed. All unwanted or duplicate papers containing PHI will be shredded immediately after it is determined that they are no longer needed. Diskettes and hard drives containing protected health information must be reformatted when the data is no longer required.

2.26 *Information* - Because of the complexity of the HIPAA Act requirements, the Privacy Officer is available to assist in responding to questions about the coverage and meaning of the City's HIPAA Privacy Policy. You may contact: Kevin Bratton, Director of Human Resources, Privacy Officer, 601 East Main Street, Johnson City, TN 37601.

3.0 RESPONSIBILITY: The Human Resources Director is responsible for the administration and communication of this policy.

APPROVED:

_____
M. Denis Peterson
City Manager

Original: 04/10/2003
Revisions: