CITY OF BIG BEAR LAKE

HIPAA PRIVACY
POLICIES AND PROCEDURES

Effective April 14, 2004

TABLE OF CONTENTS

STATEMENT OF PURPOSE

On August 14, 2002, the U.S. Department of Health and Human Services (HHS) published final regulations for Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule). The Rule was established to provide national standards for the protection and privacy of protected health information (PHI).

The purpose of this document is the establishment of the Health Insurance Portability and Accountability Act (HIPAA) Policies and Procedures for employees of the City of Big Bear Lake ("City"). This Administrative Regulation will be effective April 14, 2004. This document provides a comprehensive outline of what the City employees' responsibilities will be to be in compliance with Federal and State HIPAA Privacy Regulations.

PRIVACY OFFICER

The Administrative Services Director (currently Kathleen Smith) or designee serves as the Privacy Officer. The Privacy Contact is the HR Administrative Secretary, currently Ginny Hellerud.

The Privacy Officer's primary responsibilities include:

- development of the HIPAA Privacy Policies and Procedures;
- oversight of the HIPAA Privacy Policies and Procedures implementation;
- preparation and oversight of distribution of the HIPAA Privacy Notice;
- development, coordination and participation in the education and training for managers and Human Resources Department staff;
- development of an atmosphere to encourage associates to report possible noncompliance by the City, health insurance carriers and/or Third Party Administrators (TPA);
- acting on matters related to privacy compliance. This includes the design and coordination of internal reviews and any needed corrective action (e.g., revisions to HIPAA Privacy Policies and Procedures, institution of additional training);
- coordination with the Human Resources Department for disciplinary sanctions associated with violations of the HIPAA Privacy Policies and Procedures;
- coordination of mitigating efforts in the event of a violation to the Privacy Rules; and
- periodic revision of the HIPAA Privacy Policies and Procedures as a result of changes of City, Federal or State law.

PRIVACY PRACTICES

USES AND DISCLOSURES OF PHI

Health care carriers, third party administrators and our Plan may use and disclose personal health information (PHI) without a written authorization from the employee for the purposes listed below:

Treatment: The plan may disclose PHI to a health care provider who renders treatment on an employee's behalf. For example, if the employee is unable to provide his/her medical history as the result of an accident, the Plan may advise an emergency room physician about any allergies to medications that he/she may have.

Payment: The Plan may use and disclose PHI so claims for health care treatment, services, and supplies receive from health care providers may be paid according to the Plan's terms. For example, the Plan may receive and maintain information about surgery received to enable the processing of a hospital's claim for reimbursement of surgical expenses incurred on the employee's behalf.

Health Care Operations: The Plan may use and disclose PHI to enable it to operate or make certain all of the Plan's participants receive their health benefits. For example, the plan may use PHI for case management or to perform population-based studies designed to reduce health care costs. In addition, the Plan may use or disclose PHI to conduct compliance reviews, audits, actuarial studies, and/or for fraud and abuse detection. The Plan may also combine health information about many Plan participants and disclose it to the Plan Sponsor (e.g. Blue Cross) in summary fashion so it can decide what coverages the Plan should provide. The Plan may remove information that identifies employees from health information disclosed to the Plan Sponsor so it may be used without learning who the specific participants are.

USES AND DISCLOSURES OF PHI WITHOUT AN AUTHORIZATION

Health care carriers, third party administrators and our Plan may use and disclose personal health information (PHI) without a written consent, or authorization from the employee or an opportunity to object to the use or disclosure of PHI for the purposes listed below:

As required by law: The Plan will disclose PHI when required to do so by federal, state or local law, for example, those that require the reporting of certain types of wounds or other physical injuries.

Treatment Alternatives: The Plan may use or disclose PHI to tell employees about possible treatment options or other health-related benefits that may be of interest to them. For example, a diabetic patient may be contacted about participating in an educational program to help diabetes patients manage their diets.

Plan Administration: The Plan may disclose PHI to the plan sponsor (e.g. Blue Cross) or other organizations that sponsors the group health plan to permit them to perform plan administration

functions. The Plan may also disclose PHI which does not personally identify employees or reveal the identity in some other manner.

Public Health Authorities: The Plan may disclose PHI for public health activities including preventing or control-ling disease, injury or disability; reporting births and deaths; reporting child abuse or neglect; or reporting reactions to medication or problems with medical products or to notify people of recalls of products they have been using.

Business Associates: The Plan may disclose to persons who provide services to us, but will not disclose PHI to business associates unless the Plan receives satisfactory assurance that they will comply with privacy regulations and our procedures on the use of PHI. For example, the Plan may input information about health care treatment into an electronic claims processing system maintained by the Plan's business associate so claims may be paid.

Law Enforcement: The Plan may disclose PHI if asked to do so by a law enforcement official, for example, to identify or locate a suspect, material witness, or missing person or to report a crime, the crime's location or victims, or the identity, description, or location of the person who committed the crime.

Special Government Functions: The plan may disclose PHI as required by authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law to enable them to provide protection to members of the U.S. government or foreign heads of state, or to conduct special investigations.

Judicial and Administrative Proceedings: The Plan may disclose PHI in response to a court or administrative order. We may also disclose PHI in certain cases, in response to a subpoena, discovery request or other lawful due process.

Health Oversight Authorities: The Plan may disclose PHI to health oversight authorities such as health inspectors, for activities including audits or governmental investigations, inspections, disciplinary proceedings and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the health care system and government programs.

Victims of Abuse, Neglect or Domestic Violence: The Plan may disclose PHI to government agencies about abuse, neglect or domestic violence; to report adverse events such as product defects; or to notify a person about exposure to a possible communicable disease as required by law.

Workers' Compensation: The Plan may disclose PHI to the extent necessary to comply with state laws for workers' compensation programs.

Coroners, Funeral Directors, Organ Donation: In the event of a death, the Plan may disclose the PHI of a deceased person to a coroner, medical examiner, funeral director, or organ procurement organization for certain purposes. Under certain circumstances, we may disclose PHI for research purposes, provided certain measures have been taken to protect privacy.

Correctional Institutions and Law Enforcement Custodial Situations: If an employee should become an inmate of a correctional institution or under the custody of law enforcement officials, the Plan may disclose PHI to a correctional institution or law enforcement official as authorized or required by law.

The Plan and its business associates must obtain an authorization before using or disclosing psychotherapy notes recorded by a mental health professional documenting or analyzing the contents of a conversation with an employee during private counseling sessions. This limitation does not include summary information about mental health treatment. Psychotherapy notes can be used or disclosed without an authorization if the Plan needs to defend itself in a legal action or other proceeding brought by the employee, for professional oversight of the therapist, in certain instances to a coroner or medical examiner, or if necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

RIGHTS REGARDING PHI

Right to Access PHI: The employee has the right to review or obtain copies of his/her PHI, with some limited exceptions (such as psychotherapy notes, information compiled in anticipation of a civil, criminal or administrative action or proceeding). Usually the records include enrolment, billing, claims payment and case or medical management records. To inspect and copy health information maintained by the Plan, submit a request in writing to the Plan Administrator. A fee may be charged for the costs of producing, copying and mailing requested information, but the employee must be informed of the cost in advance. In limited circumstances, the Plan may deny a request and will provide a written response. Generally, the employee may request a review of the denial.

Right to Amend PHI: If an employee feels that PHI maintained by the Plan is incorrect or incomplete, he/she may ask the Plan to amend it. To request an amendment, send a detailed request in writing to the Plan Administrator. He/she must provide the reason(s) to support a request. The Plan may deny the request if asked to amend health information that was: complete and accurate; not created by the Plan; not part of the PHI kept by or for the Plan; or not information that the employee would be permitted to inspect and copy.

Right to an Accounting of Disclosures by the Plan: Employees have the right to request an accounting of disclosures the Plan has made of PHI. This is a list of disclosures of an employee's PHI that the Plan has made to others, except for those necessary to carry out health care treatment, payment or operations, disclosures made to the employee or in certain other situations. The employee must submit a request in writing and state a time period for which he/she wants an accounting. This time period may not be longer than 6 years.

Right to Request Restrictions on the Use and Disclosure of PHI: Employees have the right to request that the Plan restrict the manner in which it uses or disclose PHI for treatment, payment or health care operations, or to restrict the information that is provided to family, friends and other individuals involved in health care. The Plan is not required to agree to requested restrictions. If the employee requests a restriction and the information that was requested to be restricted is needed to provide emergency treatment, we may use or disclose the protected health information to a health care provider who is providing emergency treatment. A request for a restriction must be made in

writing the Plan Administrator. In the request, the employee must tell us (1) what information he/she want to limit; (2) whether he/she wants to limit the Plan's use, disclosure, or both; and (3) to whom the restrictions to apply. The Plan retains the right to terminate an agreed-to restriction if the Plan believes such termination is appropriate. In the event of a termination by the Plan, the Plan will notify the employee of such termination, which will not be effective until the employee has been informed of it. Employees also have the right to terminate, in writing or orally, any agreed-to restriction.

Right to Receive Confidential Communications: Employees have the right to request that the Plan use a certain method to communicate with him/her or information be sent to a certain location if a communication could endanger the employee. To request confidential communications, the employee must make a request in writing to the Plan Administrator and clearly state that all or part of the communication from us could endanger him/her. We will attempt to accommodate all reasonable requests. The employee must specify how or where he/she wishes to be contacted.

USES OR DISCLOSURES WITH AN AUTHORIZATION

PHI may be disclosed with an authorization from individuals. For example, a request for assistance in reconciling billings or an Explanation of Benefits. The purpose of the disclosure must be stated on an Authorization for Disclosure of Protected Health Information. The employee may revoke an authorization at any time in writing, except to the extent that we have already taken action on the information disclosed or if we are permitted by law to use the information to contest a claim or coverage under the plan. The employee must contact the Privacy Contact for an authorization form to begin the process.

USES OR DISCLOSURES WTH A CONSENT

The use or disclosure of PHI with a written consent form will be required for the release of the examination and/or test results to representatives of the City for review and use in the decision-making process regarding employment, substance abuse testing, etc.

USES AND DISCLOSURES WITH AN OPPORTUNITY TO CONSENT OR OBJECT

A covered entity as defined below may use or disclose PHI without the individual's consent or authorization for facility directories, to family members and others involved in the individual's care, or for disaster relief purposes. However, the individual must be informed in advance and given the opportunity to agree, prohibit, or restrict the disclosure or use.

SAFEGUARDS

ADMINISTRATIVE SAFEGUARDS

The City has trained its Human Resources employees on the HIPAA Privacy Policies and Procedures. Those employees are required to use all reasonable measures to safeguard individuals' PHI. In addition, Business Associates Agreements are in place with those organizations with which there will be communications regarding PHI.

The offices of the Human Resources Department are enclosed for confidential discussions and are keyed differently from the remainder of the Civic Center. Keys are provided only to the HR personnel, the City Manager and the Facilities Maintenance Worker II. Also, the HR Department has a dedicated facsimile machine to which only HR personnel have access.

TECHNICAL SAFEGUARDS

With the exception of workers' compensation information (to which HIPAA does not apply), the City does not keep PHI in electronic form, including accessing or distributing PHI via e-mail. PHI (other than workers' compensation information) is not kept on individual personal computers or on the City's server. The results of pre-employment physicals and drug testing include only whether or not the employee is able to perform the job functions and does not specify any additional detail. In the event correspondence containing PHI is forwarded to the City or from the City to a carrier, business associate or TPA it will be sent via the dedicated facsimile machine located in the Human Resources office or via U.S. mail, Fedex, etc. Telephone lines are confidential and office doors are kept closed for conversations involving PHI.

PHYSICAL SAFEGUARDS

The following safeguards are currently in place. All files containing PHI are kept separate from other employment files, are kept locked in a separate room with restricted access and locks on the file cabinets. Documents and files are not left unattended on desks or in offices at any time, and automatic screensavers are set for two minute intervals from the cessation of desktop work.

MINIMUM NECESSARY

Any time PHI is requested by another covered entity, the City will make reasonable efforts to limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. Routine recurring disclosures or requests for disclosures will be reviewed to determine that the PHI disclosed is the minimum amount reasonably necessary to achieve the purpose of the disclosure. For disclosures or requests that are out of the ordinary, the City's Privacy Officer or designee will review each disclosure individually to ensure that it is in compliance with the minimum amount necessary.

Routine and recurring disclosures may include information regarding:

1. Employee requests for assistance with medical billing issues:
    a. are to be referred to insurance broker where feasible (who is obligated under the terms of our Business Associates Agreement), who will obtain a written authorization for employee and coordinate directly as a liaison with the health carrier and the employee; or
    b. HR staff will obtain a written authorization from the employee and coordinate directly as a liaison with the health carrier and the employee;
2. Life/long term disability insurance enrollment forms including health statements (no other insurance enrollment forms request personal health information);

3. Physicians' notes received: we request only information regarding the employee's ability to perform the required job functions without detailed medical information;
4. FMLA medical certifications are to be limited to physician's notes. We request only information regarding the employee's ability to perform the required job functions without detailed medical information.
5. Workers' compensation claims, to which HIPAA rules do not apply;

Communications between the City, health carriers, TPAs and Business Associates are to be made via telephone, facsimile or U.S. mail, as well as communications with employees and their dependents. All communications will be limited to the minimum amount reasonably necessary to achieve the purpose of the disclosure.

RETENTION OF PHI

All records pertaining to PHI are retained indefinitely. Safeguard procedures as listed above for the protection of records are followed as detailed above.

DOCUMENTATION

The City will maintain the policies and procedures in written form. A copy of the policies and procedures will be posted in the Civic Center and on the website. Any communications required to be in writing will be maintained either in writing or an electronic copy as documentation.

VERIFICATION OF INDENTITY

If the City is planning to disclose PHI, it will verify the identity of the person making the request, establish his/her authority to have access to the information, and obtain any corresponding documentation. In the event of personal knowledge of the requestor, that shall be considered adequate verification of identity.

EDUCATION AND TRAINING

All City employees with access to PHI have been trained prior to the effective date of HIPAA Privacy regulations, April 14, 2004, on the City's HIPAA Privacy Policies and Procedures. All new employees who have access to PHI will be trained on the City's HIPAA Privacy Policies and Procedures within a reasonable period after orientation.

The City will update the HIPAA Privacy Policies and Procedures as needed to be in compliance with Federal and State regulations.

COMPLAINT PROCESS

The City is committed to complying with HIPAA Federal and State privacy laws and to correct any violations whenever they may occur in the organization. Each individual has the responsibility to report to the City's Privacy Officer, and/or to the City's Health Care Carriers or Third Party Administrators, any activity that violates applicable privacy laws, rules, regulations or the City's HIPAA Privacy Policies and Procedures.

The City's Privacy Officer, Health Care Carriers and Third Party Administrators will assist individuals who have questions regarding their privacy rights or who want to report a privacy breach. Any individual may contact the City's Privacy Officer, or Health Care Carrier's Privacy Office and/or Third Party Administrator's Privacy Officer to file a complaint over a possible breach of privacy regulations. A log will be maintained of reported violations, the nature of any investigation and its results, including mitigation measures taken. Individuals also have the right to report violations to the Secretary of the Department of Health and Human Services.

The City will make every effort to maintain the confidentiality of the identity of any individual who reports possible violations, although there may be a point at which an individual's identity becomes known or must be revealed as a legal matter.

There will be **no retaliation** against an individual who reports a possible violation of: Federal or State privacy regulations, the City's HIPAA Privacy Policies and Procedures, or his or her privacy rights.

MITIGATION PROCEDURES

If a use or disclosure by the City or the City's business associate(s) would violate HIPAA Privacy regulations, the City will take prompt action to mitigate any damaging effects that the disclosure could have on a participant(s). The City's employees are required to report any violation that they observe, or learn of, to the City's Privacy Officer, so that the action to mitigate the damage, if any, can commence promptly.

DETECTION OF OFFENSES AND IMPLEMENTATION OF CORRECTIVE ACTIONS

The City and its business associates will immediately address any possible violations of HIPAA Privacy regulations and/or privacy procedures.

Investigation and Corrective Actions If the City receives a report of noncompliance, or the Privacy Officer or a business associate of the City discovers credible evidence of a violation, an investigation will immediately ensue. It is the City's and its business associates' policy to institute corrective action upon identification of a violation.

Systematic Changes to Correct Violations After a problem has been identified and corrected, the Privacy Officer and, if applicable, business associates of the City will review the circumstances to determine:

1) Whether similar problems have been identified elsewhere;
2) Whether modifications to the City's HIPAA Privacy Policies and Procedures and/or business associates' policies and procedures are necessary to prevent and detect other inappropriate conduct or violations of privacy rules and/or procedures.

The Privacy Officer will work with, if applicable, business associates to avoid future violations.

DISCIPLINARY SANCTIONS

All violators of the HIPAA Privacy Policies and Procedures will be subject to disciplinary action. The precise discipline will depend on the nature and severity of the violation. Any employee who fails to comply with the City's HIPAA Privacy Policies and Procedures will be subject to discipline as established in the City's Personnel Rules and Regulations.

MODIFICATIONS TO HIPAA PRIVACY POLICIES AND PROCEDURES

Examples of when the HIPAA Privacy Policies and Procedures must be modified:

- Notification is received from broker, newsletter, or another source of a modification to Federal or State HIPAA laws.
- A flaw is found in the existing HIPAA Privacy Policies and Procedures.
- The carrier or TPA has made a change in their policy that will affect the HIPAA Privacy Policies and Procedures.

HIPAA CHECKLIST FOR NEW EMPLOYEES

The Human Resources Department has certain responsibilities to ensure HIPAA compliance for newly hired employees. These responsibilities are:

- Providing the initial HIPAA Privacy Notice to any employee who is eligible to participate in a group health plan, regardless of whether the employee enrolls or not. The Notice will be posted on the website.

- Providing new employees with a copy of the HIPAA Privacy Policies and Procedures. These will also be posted on the website.

DEFINITIONS

Whenever used, the following terms have the following meaning unless a different meaning is clearly required by the context:

Authorization: To allow use and disclosure of PHI for purposes other than treatment, payment or health care operations by both the covered entity requesting the information and a third party.

Business Associate: A person (including a vendor or other entity) who is not an employee of covered entity and either performs or assists in a function involving the use or disclosure of Individually Identifiable Health Information (IIHI) (including certain insurance functions, such as claims processing, data analysis, utilization review and billing) or provides certain services to the covered entity (including accounting, actuarial, administrative and legal) which includes the receipt or disclosure of IIHI. A covered entity may be a business associate of another covered entity.

Covered Entity: This consists of (1) health plans, which includes health, dental, vision, prescription drug insurers, HMOs, long-term care insurers and employer sponsored group health

plans; (2) health care clearinghouses, an entity that processes nonstandard information received from another entity into a standard format, including billing services; and (3) any health care provider who transmits health information in electronic form, including hospitals, physicians, dentists and other practitioners and providers of medical or health services.

Individually Identifiable Health Information (IIHI): Health information that is a subset of health information, including demographic information collected from an individual, and is (1) created or received by a health care provider, health plan, employer, 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; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Health Care Carrier: A health care carrier is an individual or group plan that provides or pays for the cost of medical care. This includes the following in one or any combination: a group health plan, a health insurance issuer, an HMO, Part A or Part B of the Medicare program, the Medicaid program, an issuer of a Medicare supplemental policy, an issuer of a long-term care policy (excluding a nursing home fixed indemnity policy), an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

Privacy Officer: An employee of the City of Big Bear Lake who has the responsibility of developing and implementing HIPAA Privacy Policies and Procedures to ensure the City's compliance with the Privacy Rule.

Protected Health Information (PHI): Individually identifiable health information that is transmitted by electronic media, maintained in any electronic medium, or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act, and employment records held by a covered entity in its role as employer.

Third Party Administrator: An entity that may collect premiums, pay claims and/or provide administrative services to the City's group benefits program.

MARKETING PROTOCOL FOR HEALTH CARE BENEFITS

The procedures described below must be followed when providing census information to brokers or forwarding census information to carriers in order to market any of the following health care benefits:

- Medical
- Dental
- Vision
- Prescription Drug Coverage
- EAP
- Mental Health and Substance Abuse Benefits
- Long Term Care Benefits

All census data collected to market healthcare benefits must be limited to the following fields:

1. Date of Birth
2. Gender
3. Coverage Type
4. Coverage Tier
5. Zip code

The following identifying factors may **not** be provided when forwarding census information:

- Employee's Name
- Employee's Last Name
- Social Security Number
- Employee's ID Number (used by the employer and/or TPA or insurance carrier)
- Employee's full address (may use city, state, and zip code)

CENSUS DATA FOR HEALTH CARE BENEFITS

City of Big Bear Lake
Census (Example)

DATE OF BIRTH	GENDER	COVERAGE TYPE [1]	PLAN TYPE [2]	COVERAGE TIER [3]	STATUS[4]	CLASS [5]	ZIP CODE
01/17/1960	F	Medical	HMO	EE only	Active	Full Time	91509

1 COVERAGE TYPE: Medical, Dental, Vision, etc.
2 PLAN TYPE: HMO, PPO, POS, OOA, Other
3 COVERAGE TIER: EE only, EE + family
4 STATUS: Active, COBRA, Disability, Other
5 CLASS: Full-Time or Part-Time

MARKETING PROTOCOL NON-HEALTH CARE BENEFITS

The procedures described below must be followed when requesting census information from clients and prospects or forwarding census information to carriers in order to market any of the non-health care benefits listed below.

- Life
- Long Term Disability (LTD)
- Short Term Disability (STD)
- Accidental Death and Dismemberment (AD&D)
- Business Travel Accident (BTA)
- Voluntary Plans

All census data collected to market non-healthcare benefits must be limited to the following fields:

1. Date of Hire
2. Date of Birth
3. Gender
4. Zip Code
5. Annual Salary
6. Current Benefit Coverage
7. Job Title or Class
8. Zip Code

The following identifying factors may **not** be forward to a broker or carrier when providing census information:

- Employee's Name
- Employee's Last Name
- Social Security Number
- Employee's ID Number (used by the employer and/or TPA or insurance carrier)
- Employee's full address (may use city, state, and zip code)

MARKETING PROTOCOL NON-HEALTH CARE BENEFITS - continued

CENSUS FOR NON-HEALTH CARE BENEFITS

City of Big Bear Lake **Census (Example)**						
DATE OF HIRE	**DATE OF BIRTH**	**GENDER**	**ANNUAL SALARY**	**CURRENT BENEFIT COVERAGE**	**JOB TITLE OR CLASS**	**ZIP CODE**
11/01/2000	01/17/1952	M	$50,000	1 x salary	Systems Adm.	90679