CITY OF SAN MATEO

(Self insured plans)

HIPAA PRIVACY
POLICIES AND PROCEDURES

EFFECTIVE APRIL 14, 2004

HIPAA
PRIVACY POLICIES AND PROCEDURES

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 individually identifiable health information.

The purpose of this document is the establishment of HIPAA Policies and Procedures for employees of ***CITY OF SAN MATEO***. These policies and procedures will be effective April 14, 2004. This document will provide a comprehensive outline of what ***CITY OF SAN MATEO*** employee's responsibilities will be to be in compliance with federal and state HIPAA Privacy Regulations.

DEFINITIONS

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

Authorization: To allow use and disclosure of protected health information 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: An entity subject to HIPPA Privacy Rules, which may cover more components than just health care components and must ensure it does not disclose protected health information to another component of the entity that would be prohibited from receiving information.

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.

- is either created or received by a health care provider, health plan, employer or health care clearinghouse; and
- relates to an individual's physical or mental health (past, present, or future), or the health care or payment for health care of the individual.

The information must either identify the individual or be capable of being 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, in 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 a covered entity (employer group) who has the responsibility of developing an implementing policies and procedures to ensure the covered entity's compliance of the Privacy Rule.

Privacy Committee: A committee composed of employees of a covered entity (employer group) whose purpose is to assist the Privacy Officer with the development, implementation and enforcement of Privacy Policies and Procedures and HIPAA Privacy Rules.

Protected Health Information (PHI): Is 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 OF SAN MATEO*** Group Benefits Program.

PRIVACY OFFICER AND PRIVACY COMMITTEE

The Employee Benefits Committee appoints the Privacy Officer. Documentation of this appointment must be retained for six years from the date that the appointment is in effect.

The Privacy Officer's primary responsibilities include:

- development of the Privacy Program policies and procedures;
- oversight of the Privacy Program implementation;
- preparation and oversight of distribution of the Notice of Privacy Practices;
- reporting on a regular basis (indicate reporting authority) on the progress of ***City of San Mateo's*** implementation and compliance;
- development, coordination and participation of the education and training for associates and managers;
- development of an atmosphere to encourage associates to report possible noncompliance of ***CITY OF SAN MATEO***, health insurance carriers and Third Party Administrators;
- acting on matters related to privacy compliance. This includes the design and coordination of internal reviews and any needed corrective action (e.g., revise policies and procedures, institute additional training);
- coordination with the human resources office for disciplinary sanctions associated with violations of the Privacy Program, policies and procedures;
- coordination for mitigating efforts in the event of a violation to the Privacy Rules; and
- periodic revision of the Privacy Program's policies and procedures as a result of changes at ***CITY OF SAN MATEO***, federal or state law.
- The Privacy Officer shall oversee the HIPAA Privacy and Security and be responsible for the implementation of the Privacy Program.

CITY OF SAN MATEO **CORPORATE PRIVACY COMMITTEE**		
NAME	**TITLE**	**CONTACT INFORMATION**
Colleen Nolan	Privacy Officer	CNOLAN@cityofsanmateo.org
Dennis Caines	Committee Member	DCAINES@cityofsanmateo.org
Evelyn Walker	Committee Member	EWALKER@cityofsanmateo.org

The Privacy Committee's responsibilities will include:

- recommending and monitoring, in conjunction with the relevant business units or departments, the development of internal systems to carry out the privacy policies and procedures as part of daily operations;
- determining the appropriate strategy/approach to promote compliance with the Privacy Program and detection of any potential violations, such as through hotlines and other reporting mechanisms;
- developing a system to solicit, evaluate and respond to complaints and problems; and
- monitoring ongoing operations for the purpose of identifying potentially deficient areas and implementing corrective and preventive action.

When a potential problem is identified, the Privacy Officer may also select various individuals to serve on an ad hoc task force to provide assistance in investigating an incident, such as an unauthorized disclosure, implementing mitigation measures and/or designing protocols to prevent a recurrence in the future.

COMPLAINT PROCESS

CITY OF SAN MATEO 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 ***CITY OF SAN MATEO'S***' Privacy Officer, Privacy Committee, and/or to ***CITY OF SAN MATEO*** Health Care Carriers or Third Party Administrators, any activity that violates applicable privacy laws, rules, regulations or ***CITY OF SAN MATEO*** privacy policies and procedures.

CITY OF SAN MATEO'S Privacy Officer, Privacy Committee, 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 ***City of San Mateo's*** Privacy Officer, Privacy Committee 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.

CITY OF SAN MATEO 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, ***CITY OF SAN MATEO*** privacy policies and procedures, or his or her privacy rights.

MITIGATION PROCEDURES

If a use or disclosure by ***CITY OF SAN MATEO*** or ***CITY OF SAN MATEO'S*** business associate(s) would violate HIPAA Privacy regulations or ***CITY OF SAN MATEO*** Privacy Policies and Procedures; ***CITY OF SAN MATEO*** will take prompt action to mitigate any damaging effects that the disclosure could have on a participant(s). ***CITY OF SAN MATEO'S*** employees are required to report any violation that they observe, or learn of, to ***City of San Mateo's*** Privacy Officer, Privacy Committee, or ***CITY OF SAN MATEO***, so that the action to mitigate the damage, if any can commence promptly.

DETECT OFFENSES AND IMPLEMENT CORRECTIVE ACTIONS

CITY OF SAN MATEO and its business associates will immediately address any possible violations of HIPAA Privacy regulations and/or privacy procedures.

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

Systemic Changes to Correct Violations After a problem has been identified and corrected, the Privacy Officer, Privacy Committee, ***CITY OF SAN MATEO***, and if applicable, business associates of ***CITY OF SAN MATEO*** will review the circumstances to determine:

1) Whether similar problems have been identified elsewhere
2) Whether modifications to ***CITY OF SAN MATEO*** 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.
3) The Privacy Officer will work with the Privacy Committee, and if applicable, business associates to implement changes throughout the company to avoid future violations.

DISCIPLINARY SANCTIONS

All violators of the Privacy Program or the policies and procedures will be subject to disciplinary action. The precise discipline will depend on the nature and severity of the violation.

A. DISCIPLINARY GUIDELINES: Any employee who fails to comply with ***CITY OF SAN MATEO*** Privacy policies and procedures will be subject to discipline. Such discipline may include 1) an oral or written warning; 2) reprimand; 3) suspension; or 4) termination, depending on the degree of wrongdoing, whether there have been past violations, and on the individual's cooperation in promptly reporting the incident to the appropriate manager or to the Privacy Officer. Intentional or reckless noncompliance will subject violators to significant sanctions.

B. CONSISTENT ENFORCEMENT POLICY: The range of disciplinary standards for improper conduct will be consistently applied and enforced, all personnel will be treated equally, and disciplinary action will be taken on a fair and equitable basis. Corporate officers and managers must comply with, and take action to assure that their subordinates comply with, the applicable policies and procedures.

C. EDUCATION ON DISCIPLINARY GUIDELINES: In the training sessions, all associates will be advised of the policy regarding disciplinary actions for noncompliance.

PHYSICAL AND ELECTRONIC SAFEGUARDS

CITY OF SAN MATEO has developed and implemented physical and electronic safeguards to ensure the protection of employees' protected health information.

PHYSICAL SAFEGUARDS

CITY OF SAN MATEO has implemented physical safeguards to safeguard protected health information (PHI) that it receives in paper form. ***CITY OF SAN MATEO*** has trained its employees who access or disclose PHI to third parties, on the policies and procedures they are required to follow to assure that they use all reasonable measures to safeguard individuals' PHI. ***CITY OF SAN MATEO'S*** employees are restricted from making any uses or disclosures of PHI that would violate ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Procedures and/or HIPAA Privacy regulations.

ELECTRONIC SAFEGUARDS

CITY OF SAN MATEO has implemented technical safeguards to assure the protection of PHI collected in electronic form. ***CITY OF SAN MATEO*** has implemented firewalls, role-base access and the use of password protections to restrict access to individuals who do not need to use or distribute employees' PHI to perform their job functions. ***City of San Mateo's*** employees have received training on the restrictions on accessing or distributing PHI via e-mail. ***City of San Mateo's*** employees will only respond to e-mails that contain PHI, if the individual who sends or receives the PHI acknowledges the risk to privacy inherent in the use of e-mail communications, and authorizes ***CITY OF SAN MATEO*** to send the PHI to the individual's verified e-mail address.

EDUCATION AND TRAINING

All ***CITY OF SAN MATEO*** employees with access to PHI have been trained prior to the effective date of HIPAA Privacy regulations, April 14, 2004, on the ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Procedures.

All employees with access to PHI will be required to attend and participate in HIPAA Privacy training seminars. ***CITY OF SAN MATEO*** maintains attendance logs of the training seminars attended by employees who access PHI and will use this information in the annual evaluation process of each employee.

All new employees who access PHI will be trained on ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Procedures within a reasonable period after orientation.

CITY OF SAN MATEO will periodically update the ***CITY OF SAN MATEO*** HIPAA Policies and Procedures, as its operations change or as the result of the enactment of new federal or state statutes on HIPAA Privacy. ***CITY OF SAN MATEO*** will distribute the updated policies and procedures, notify employees of the changes, if applicable, and provide additional training to assure that employees accessing PHI understand the modifications to ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Procedures.

APPENDIX A

MODIFICATIONS TO HIPAA POLICIES AND PROCEDURES

The following form should be used when changing your existing HIPAA policies and procedures. This form will assist you in keeping a chronology of the modifications to your policies and procedures.

Examples of when policies and procedures must be modified:

- You have received notification from broker, newsletter, or another source of a modification to federal or state HIPAA laws.
- You have found a flaw in your existing policies procedures.
- Your carrier or TPA has made a change in their policy that will affect your policies and procedures.

How to Modify a Policy of Procedure

1. Review with legal counsel new state and/or federal regulatory requirements, and/or new TPA/carrier policies and procedures.
2. Assess how existing policies and procedures are impacted by new legislation or new carrier/TPA policies and procedures (i.e., monetary, security, etc.).
3. Determine if revised Privacy Notice is required.
4. Draft new policies and procedures (Privacy Officer and Legal Counsel).
5. Adopt new policies and procedures (Privacy Officer).
6. Record new procedure on enclosed form.
7. Train Human Resources and appropriate staff
8. Post new policies and procedures.
9. Distribute revised Privacy Notice (if applicable)

CITY OF SAN MATEO
MODIFICATION TO POLICIES AND PROCEDURES
[SAMPLE]

Modification	Purpose of Modification	Modification Adopted by	Adoption Date	Training Completion Date	Notification (If Applicable)
Deleted use of authorization forms; pgs 9 & 10 of handbook	*Adopt amendment to HIPAA Privacy laws, Title VI, Sec. 164.520*	*John Doe, Privacy Officer Jane Smith, ABC Legal Counsel*	*1/1/2005*	*1/15/2005*	*1/30/2005 e-mailed to all employees*

SAMPLE HIPAA CHECKLIST FOR NEW EMPLOYEE/OPEN ENROLLMENT

NEW HIRES

A human resource professional has certain responsibilities to ensure HIPAA compliance for newly hired employees. These responsibilities are:

- Providing the initial HIPAA Notice to any employee who is eligible to participate in a group health plan, regardless of whether the employee enrolls or not. This Notice must describe an employee's enrollment rights and the right to receive creditable coverage for any pre-existing condition exclusion that may exist in a group health plan.

- Providing an employee with an Authorization Form to sign. Once this Form has been completed, the employee should be provided a copy, while the employer retains the original in the employee file.

- Providing an employee with the information on where they may obtain a copy of Privacy Rules procedures.

- Providing an employee with an updated summary plan description, that contains HIPAA language.

OPEN ENROLLMENT

Because most Authorizations will be valid for only a period of one year, each year at open enrollment, the human resource professional should ensure the participants of group health plans (health, dental, vision, EAP, prescription) have signed a new Authorization Form.

Remember:

If there is a change in federal or state law that will result in Privacy Rule Changes, new Privacy Rule Notifications must be distributed to employees no later than 60 days from the modification. The Notifications should be distributed in such manner that you will be able to confirm the employee receipt.

SAMPLE SIGN-IN SHEET FOR HIPAA TRAINING

Use the following form each time you conduct meetings for HIPAA training. Retain this form in your files.

CITY OF SAN MATEO
SIGN-IN SHEET
FOR HIPAA TRAINING
(Training Date)
[SAMPLE]

NAME	DEPARTMENT	SIGNATURE

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:

- Marketing Healthcare 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

You may **not** provide any of the following identifying factors 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)

Failure to comply with this procedure will violate ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Requirements and will result in disciplinary sanctions.

CENSUS DATA FOR HEALTH CARE BENEFITS

CITY OF SAN MATEO Census [SAMPLE]							
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 + spouse, 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
- Short Term Disability (STD)
- Long Term Disability (LTD)
- Accidental Death and Dismemberment (AD&D)
- Voluntary Plans
  - STD
  - LTD
  - AD&D
  - Life

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

You may **not** forward to a broker or carrier any of the following identifying factors 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)

Failure to comply with this procedure will violate ***CITY OF SAN MATEO*** HIPAA Privacy Policies and Requirements and will result in disciplinary sanctions.

CENSUS FOR NON-HEALTH CARE BENEFITS

CITY OF SAN MATEO
Census
[SAMPLE]

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