

# City of Stockton, CA

# HIPAA Privacy Policy and Procedure Manual

## Cover Page

---

---

This HIPAA Privacy Manual is adopted and established by the City of Stockton group health plan.

This manual also includes edits to assist the Plan in complying with the Final Rule issued by the U. S. Department of Health and Human Services, modifying the Privacy, Security, Breach Notification and Enforcement Rules under the Health Insurance Portability and Accountability Act (HIPAA) published in the January 25, 2013 Federal Register, titled: *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Nondiscrimination Act (GINA); Other Modifications to the HIPAA Rules*. (The Final Rule is located here: <http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf> and is effective for this Plan on September 23, 2013.)

Throughout these policies and procedures, the following terms are used liberally and defined below:

- **Plan means** the group health plan consisting of these benefits: **self-funded medical plan options including outpatient prescription drug benefits and health reimbursement account (HRA), self-funded dental plan, self-funded vision plan, Independent Review Organizations for External Reviews, COBRA administration, and Health Flexible Spending Account (FSA) administration sponsored by the City of Stockton.**

The Plan is the **covered entity**. The Plan may contract with various Business Associates to assist in administering the Plan.

For purposes of this HIPAA Privacy Policy and Procedure Manual, the Plan does not include any fully insured medical, dental or vision plan options.

- **Hybrid Entity:** For purposes of complying with the HIPAA Privacy rules, this Plan is a “hybrid entity” because it has both group health plan functions (a health care component of the entity) and non-group health plan functions. The Plan designates that its health care group health plan functions are covered by the privacy rules. The health care group health plan functions include the “Plan” as defined above.

This Plan, as the covered entity that is a hybrid entity, will ensure that the health care component of the covered entity (meaning the group health plan) complies with the applicable requirements of section 164.105. In particular, and without limiting this requirement, our group health Plan will ensure that:

- A. Its health care component does not disclose protected health information to another component of the covered entity in circumstances that prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;
- B. Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required to protect such information if the health care component and the other component were separate and distinct legal entities;
- C. If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by HIPAA Privacy regulations.

- This Plan does not consider itself a **small health plan**.
- **PHI means** protected health information. **Protected health information** refers to individually identifiable health information that is:
  - (a) Transmitted or maintained by or in electronic media; or
  - (b) Transmitted or maintained in any other form or medium by a covered entity. (**Covered entity** means a health plan, health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulation.)

**Protected health information (PHI) does not include** individually identifiable health information in:

- (a) Education records covered by the Family Educational Right and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
- (b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv) (FERPA records on students 18 and over); and
- (c) Employment records held by a covered entity (e.g. the “Plan”) in its role as an employer such as records maintained in compliance with OSHA, Family and Medical Leave Act (FMLA), workers' compensation, and alcohol and drug free workplace laws, and
- (d) Reference to a person who has been deceased for more than 50 years.

- **Health plan** means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

1. Health plan includes the following, singly or in combination:

- i. A **group health plan**, as defined in this section.
- ii. A health insurance issuer, as defined in this section.
- iii. An HMO, as defined in this section.
- iv. Part A or Part B of the Medicare program under title XVIII of the Act.
- v. The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
- vi. The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.
- vii. An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
- viii. An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.
- ix. 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.
- x. The health care program for uniformed services under title 10 of the United States Code.
- xi. The veterans' health care program under 38 U.S.C. chapter 17.
- xii. The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
- xiii. The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
- xiv. An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
- xv. The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
- xvi. A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
- xvii. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

2. **Health plan excludes:**

- i. Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
- ii. A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):
  - A. Whose principal purpose is other than providing, or paying the cost of, health care; or
  - B. Whose principal activity is the direct provision of health care to persons; or the making of grants to fund the direct provision of health care to persons.

- **Plan Sponsor** means the **City Council/City Manager** for the City of Stockton, California.

- **Security Officer** means the **Information Technology Officer** for the City of Stockton, California.

- **Privacy Officer means** the **Deputy Director of Human Resources – Risk & Benefits** for the City of Stockton, California.

Questions or comments about the policies and procedures in this manual should be referred to the Plan's Privacy Officer at:

<p><b>City of Stockton Deputy Director of Human Resources – Risk &amp; Benefits</b> 400 E. Main Street 3<sup>rd</sup> Floor Stockton CA, 95202 Telephone: 209-937-8233 Confidential fax #: 209-937-5702</p>
---

## TABLE OF CONTENTS

HIPAA PRIVACY POLICY AND PROCEDURE ON PRIVACY NOTICES .....	6
HIPAA Notice of Privacy Practices.....	9
Form to Revoke a Personal Representative.....	16
SAMPLE HIPAA PRIVACY NOTICE COVER MEMO.....	17
SAMPLE COMBINED HIPAA PRIVACY AND WHCRA NOTICE.....	18
HIPAA PRIVACY POLICY AND PROCEDURE ON THE PRIVACY OFFICER.....	19
Position Description for the Privacy Officer.....	21
HIPAA PRIVACY POLICY AND PROCEDURE FOR AUTHORIZATIONS.....	23
Authorization Form for Release of Personal Health Information (PHI).....	28
Form to Revoke/Terminate a Prior Authorization .....	29
HIPAA PRIVACY POLICY AND PROCEDURE FOR PERSONAL REPRESENTATIVES .....	30
Form to Appoint a Personal Representative.....	33
Form to Revoke a Personal Representative.....	34
HIPAA PRIVACY POLICY AND PROCEDURE FOR MINIMUM NECESSARY .....	35
HIPAA PRIVACY POLICY AND PROCEDURE FOR VERIFICATION OF IDENTITY .....	41
HIPAA PRIVACY POLICY AND PROCEDURE FOR SAFEGUARDING PHYSICAL, ADMINISTRATIVE AND TECHNICAL PHI.....	47
HIPAA PRIVACY POLICY AND PROCEDURE FOR CERTIFICATION AND PLAN DOCUMENT AMENDMENT.....	52
Certification to the Group Health Plan.....	54
PLAN DOCUMENT AMENDMENT .....	56
HIPAA PRIVACY POLICY AND PROCEDURE FOR BUSINESS ASSOCIATES.....	59
SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS .....	64
HIPAA PRIVACY POLICY AND PROCEDURE FOR USE AND DISCLOSURE OF PHI AS REQUIRED BY LAW.....	75
Request for Access to Protected Health Information (PHI) Without Authorization from an Individual .....	83
HIPAA PRIVACY POLICY AND PROCEDURE ON RECORD RETENTION AND DESTRUCTION.....	84
HIPAA PRIVACY POLICY AND PROCEDURE FOR USE AND DISCLOSURE OF PHI REQUIRING AN OPPORTUNITY FOR AN INDIVIDUAL TO AGREE OR OBJECT .....	89
HIPAA PRIVACY POLICY AND PROCEDURE ON COMPLAINTS .....	92
Privacy Complaint Form.....	95
HIPAA PRIVACY POLICY AND PROCEDURE FOR DE-IDENTIFICATION AND RE-IDENTIFICATION OF PHI .....	96
HIPAA PRIVACY POLICY AND PROCEDURE ON SANCTIONS FOR VIOLATION OF PRIVACY RULES .....	99
HIPAA PRIVACY POLICY AND PROCEDURE FOR TRAINING .....	101
City of Stockton Confidentiality Agreement .....	104
HIPAA Training Certification and Confidentiality Agreement Form .....	105

HIPAA PRIVACY POLICY AND PROCEDURE FOR USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS (TPO) .....	106
HIPAA PRIVACY POLICY AND PROCEDURE FOR MITIGATION.....	111
HIPAA PRIVACY POLICY AND PROCEDURE REGARDING ANTI-RETALIATION .....	112
HIPAA PRIVACY POLICY AND PROCEDURE DISCLOSURES OF PHI BY WHISTLEBLOWERS AND VICTIMS OF CRIME.....	113
HIPAA PRIVACY POLICY AND PROCEDURE FOR POLICIES AND PROCEDURES FOR COMPLIANCE WITH HIPAA PRIVACY REGULATIONS.....	115
HIPAA PRIVACY POLICY AND PROCEDURE ON ACCESS TO PHI.....	117
Request for Access to Protected Health Information (PHI) .....	121
Notice of Extension to Decide Request for Access to PHI .....	122
Notice of Denial of Access to PHI .....	123
HIPAA PRIVACY POLICY AND PROCEDURE ON RIGHT TO REQUEST PRIVACY PROTECTION (RESTRICTIONS) ON USE AND DISCLOSURE OF PHI .....	124
Request For Restrictions On Use And Disclosure Of PHI.....	127
Request to Revoke a Prior Restriction on Use & Disclosure of PHI .....	128
HIPAA PRIVACY POLICY AND PROCEDURE FOR REQUESTING THAT PHI BE TRANSMITTED CONFIDENTIALLY (e.g. by Alternate Means or Location).....	129
Request That PHI Be Transmitted Confidentially .....	130
Request to Terminate the Confidential Transmission of PHI .....	131
HIPAA PRIVACY POLICY AND PROCEDURE ON RIGHT TO AMEND PHI .....	132
Request to Amend Protected Health Information (PHI) .....	136
HIPAA PRIVACY POLICY AND PROCEDURE ON THE RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI .....	137
Request for Accounting of Disclosure of Protected Health Information (PHI) .....	141
HIPAA PRIVACY POLICY AND PROCEDURE FOR WAIVER OF RIGHTS .....	142
HIPAA PRIVACY POLICY AND PROCEDURE FOR LIMITED DATA SET .....	143
HIPAA PRIVACY POLICY AND PROCEDURE FOR FUNDRAISING AND UNDERWRITING .....	145
HIPAA PRIVACY POLICY AND PROCEDURE FOR MARKETING AND PROHIBITION ON SALE OF PHI .....	147
HIPAA PRIVACY POLICY AND PROCEDURE REGARDING STATE LAWS .....	152
HIPAA PRIVACY POLICY AND PROCEDURE ON NOTIFICATION IN THE CASE OF A BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI) .....	155
HIPAA INCIDENT REPORT/RISK ASSESSMENT .....	162
CHECKLIST FOR CREATION OF AN INDIVIDUAL BREACH NOTICE.....	166
SAMPLE BREACH NOTIFICATION LETTER TEMPLATE .....	167
HIPAA INCIDENT LOG .....	170
HIPAA PRIVACY POLICY AND PROCEDURE ON LIMITATIONS ON THE USE AND DISCLOSURE OF GENETIC INFORMATION.....	171



## HIPAA PRIVACY POLICY AND PROCEDURE ON PRIVACY NOTICES

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.520 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

An individual has the right to adequate notice of the Uses and Disclosure of PHI that may be made by the Plan, the rights of the individual and the duties of the Plan with respect to PHI.

- A. **Notice Distribution:** The Plan will prepare and distribute a Privacy Notice describing the Plan's privacy policies and procedures. The Notice will be provided (method of delivery discussed in the procedures section of this policy and procedure) to the "named insured" covered under the Plan at the following times:
- No later than April 14, 2003 to all covered individuals (actual receipt may vary depending on the date the notice is mailed),
  - To all new enrollees at the time of enrollment,
  - Within 60 days of a material revision in the Privacy Notice;
  - Upon request.
- B. **Notice Reminders:** No less frequently than once every three years this Plan will notify individuals (then covered by the Plan) of the availability of the Notice and how to obtain the Notice.
- C. In compliance with 164.530 (i) and 502(i) the Plan will not use or disclose protected health information in a manner inconsistent with the Privacy Notice.
- D. **Notice Content:** The content of the Privacy Notice will comply with the requirements of the HIPAA Privacy regulation at 164.520 (b). It will:
- include the required header text,
  - address uses and disclosures including at least one example of the types of uses and disclosures the Plan makes,
  - contain separate statements for certain uses and disclosures,
  - contain a description of the types of uses and disclosures that require an authorization and that an authorization may be revoked,
  - contain a statement that the Plan is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information and notify affected individuals following a breach of unsecured protected health information,
  - address an individual's rights,
  - note the Plan's duties as the covered entity,
  - address how and where to complain,
  - note the contact for further information and
  - indicate the effective date of the Notice.
- E. **Notice Revisions:** The Plan will promptly revise the Notice whenever there is a material change to the uses and disclosures, the individual's rights, the Plan's legal duties, or other privacy practices stated in the Notice. **Material changes** are changes to the uses and disclosures of PHI, an individual's rights, the duties of the Plan or other privacy practices stated in the Privacy Notice.

Distribution of the revised notice is as follows:

- A health plan that posts its Notice on its web site must prominently post the change or its revised Notice on its web site by the effective date of the material change to the Notice. Additionally the health plan must provide the revised Notice, or information about the material change and how to obtain the revised Notice, in its next annual mailing to individuals then covered by the Plan.

- A health plan that does not post its Notice on a web site must provide the revised Notice, or information about the material change and how to obtain the revised Notice, to individuals then covered by the Plan within 60 days of the material revision to the Notice.
- F. **Website and Electronic Notice obligations:** A covered entity (e.g. the Plan) that maintains a website that provides information about the Plan’s customer service or benefits, must prominently post the Notice on that website and make the Notice available electronically through the website.
- G. **E-mail Notice Distribution:** The Plan may provide the Notice to an individual by e-mail **IF** the individual agrees to electronic notice and such agreement has not been withdrawn. If the Plan knows that the e-mail transmission failed, a paper copy of the Notice is to be provided. An individual who received an e-mail transmission of a Notice retains the right to obtain a paper copy from the Plan upon request.
- H. **Documentation of Notice Distribution:** The Plan will document compliance with the HIPAA regulation’s Notice obligations by retaining copies of the Notices the Plan issues.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Material changes** are changes to the uses and disclosures of PHI, an individual’s rights, the duties of the Plan or other privacy practices stated in the Privacy Notice.
- **Named Insured** means the employee covered under the Plan.

## PROCEDURES

1. **Notice Distribution:** This Plan will satisfy the requirements of the HIPAA regulation by providing the Notice to the named insured (covered employee) of the Plan; however, employees will be encouraged to share the Notice with other family members covered under the Plan.
  - a. **Initial Notice Distribution:** Before April 14, 2003, the Plan mailed by first class US mail the Plan’s initial Privacy Notice to all named insureds who are covered under the Plan as of the date of Notice mailing.
  - b. **New Enrollee Distribution:** Each month the Privacy Officer (or the Privacy Officer’s designee) will obtain from Human Resources a list of individuals newly covered by the Plan. The Privacy Officer will then distribute a Privacy Notice to that newly covered individual. The method of distribution will be by including the Notice in the new hire packet. The Plan will retain proof of Notice distribution.
  - c. **Distribution of Revised Notice:** Whenever there is a material revision to the Privacy Notice, the Privacy Officer will distribute the revised notice as follows:
    - Because our health plan posts its Notice on its intranet site, we will prominently post the change or its revised Notice on that intranet site by the effective date of the material change to the Notice. We will also provide the revised Notice, or information about the material change and how to obtain the revised Notice, in our next annual mailing to individuals covered by the Plan.
    - Material changes are changes to the uses and disclosures of PHI, an individual’s rights, the duties of the Plan or other privacy practices stated in the Privacy Notice.  
The Plan will retain a copy of the revised Notice and Notice distribution list.
  - d. **Upon Request:** The Privacy Officer or its designee may distribute a Notice to a covered individual upon verbal or written request. The Plan will retain proof of Notice request and distribution dates.
  - e. **Reminder Every Three Years:** In order to meet the obligation to notify individuals (then covered by the Plan) of the availability of the Notice and how to obtain the Notice, this Plan has chosen to include a statement annually in Open Enrollment packets given to all individuals then covered by the Plan, that a Notice of Privacy Practices is available upon request and how to obtain it. The Privacy Officer will assure that such statement is included in Open Enrollment packets each year at the Plan’s designated Open Enrollment period.
  - f. Note that if any of the Plan’s health benefits are insured, an employee should also receive a HIPAA Privacy Notice from each insurance company/HMO vendor too. The Plan is not responsible for Privacy Notice distribution by other covered entities.
2. **Notice Content:** The Privacy Officer will assure that the content of all Notices issued by the Plan contain the required elements, as outlined in item “D” in the policy section of this policy/procedure.

3. **Notice Revisions:**

- a. All requests for revision of the Notice are to be reviewed by the Privacy Officer.
- b. No less frequently than once each year, the Privacy Officer will review the current Notice and make any necessary changes to the Notice, assuring that such changes remain in compliance with the required content obligations of the Notice.

4. **Website Notice Procedures:** This Plan maintains a website that provides information about the Plan's customer service or benefits; therefore, this Plan must prominently post the Notice on that website ([www.stocktongov.com](http://www.stocktongov.com)) and allow the printing of the Notice from the website. Human Resources will post the Notice.

- a. The Privacy Officer will notify the Human Resources Department at the time that the Plan distributes a revised paper copy Notice, that any prior version of the Notice is to be removed from the website and the new Notice is to be posted on the website promptly.
- b. The Privacy Officer will ensure that the new Privacy Notice is prominently posted and available on the website by logging into the website, assuring that the new Notice is legible and then printing and storing a copy of the newly posted Notice.

5. **E-mail Notice Procedures:** This Plan may send the Privacy Notice by e-mail to any covered individual **who agrees** to an electronic notice. The Plan must assure it receives an individual's agreement to an e-mail transmission of the Notice using the process below:

- a. If the request for an e-mail transmission comes to the Plan via e-mail, the Plan will retain a copy of that e-mail request as proof of the individual's agreement to e-mail transmission. Note that the individual may always request a paper copy of the Notice. If the Plan knows that the e-mail transmission of the Notice was **NOT** received, (for example the email bounced back with a delivery failure notice indicating it was not sent), the Plan will automatically mail a paper copy of the Notice to the covered individual.
- b. If the request for an e-mail transmission comes to the Plan in any other form (e.g. verbal, telephonic, handwritten), the Plan will e-mail the following statement to the individual:

“This Plan is required by law to obtain your agreement to receive a HIPAA Privacy Notice by e-mail transmission **BEFORE** the Plan e-mails a Notice to you. If you agree to receive an e-mail transmission of the Notice please return this e-mail to the Plan indicating you agree to an e-mail transmission of the Notice. Note that you are also able to obtain a paper copy of the Notice by contacting the City of Stockton Human Resources Office or you can print the Notice off the Benefits website at [www.stocktongov.com](http://www.stocktongov.com). Thank you for your patience in this process.”

- c. To assure that e-mail transmission of the HIPAA Privacy Notice is protected from unwanted alteration by the reader, the Plan will transmit the HIPAA Privacy Notice in an Adobe Acrobat attachment.

6. **Documentation of Notice Distribution:** The Privacy Officer will maintain a copy of all versions and revisions of the Privacy Notice, proof of e-mail acceptance of Notice transmission and any other required communication about the Notice in accordance with the Plan's Record Retention Policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.520
- The Plan's Privacy Officer.

**City of Stockton**  
**HIPAA Notice of Privacy Practices**

---

---

Este aviso está disponible en Español si lo solicitas. Por favor contacte el oficial de privacidad indicado a continuación.

***Purpose of This Notice***

**This Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.**

This Notice is required by law.

The City of Stockton’s self-funded group health plan encompassing the self-funded medical plan options including outpatient prescription drug benefits and health reimbursement account (HRA), self-funded dental plan, self-funded vision plan, Independent Review Organizations for External Reviews, COBRA administration, and Health Flexible Spending Account (FSA) administration (hereafter referred to as the “Plan”), is required by law to take reasonable steps to maintain the privacy of your personally identifiable health information (called **Protected Health Information or PHI**) and to inform you about the Plan’s legal duties and privacy practices with respect to protected health information including:

1. The Plan’s uses and disclosures of PHI,
2. Your rights to privacy with respect to your PHI,
3. The Plan’s duties with respect to your PHI,
4. Your right to file a complaint with the Plan and with the Secretary of the U.S. Department of Health and Human Services (HHS),
5. The person or office you should contact for further information about the Plan’s privacy practices,
6. To notify affected individuals following a breach of unsecured protected health information.

PHI use and disclosure by the Plan is regulated by the Federal law, Health Insurance Portability and Accountability Act, commonly called HIPAA. You may find these rules in 45 *Code of Federal Regulations* Parts 160 and 164. This Notice attempts to summarize key points in the regulation. The regulations will supersede this Notice if there is any discrepancy between the information in this Notice and the regulations. The Plan will abide by the terms of the Notice currently in effect. The Plan reserves the right to change the terms of this Notice and to make the new Notice provisions effective for all PHI it maintains.

You may receive a Privacy Notice from a variety of the insured group health benefit plans offered by the City of Stockton Each of these notices will describe your rights as it pertains to that plan and in compliance with the Federal regulation, HIPAA. This Privacy Notice however, pertains to your protected health information related to the City’s self-funded health benefit plan (the “Plan”) and outside companies contracted to help administer Plan benefits, also called “business associates.”

**Effective Date**

The effective date of this Notice is **November 3, 2014**, and this notice replaces notices previously distributed to you.

**Privacy Officer**

The Plan has designated a Privacy Officer to oversee the administration of privacy by the Plan and to receive complaints. The Privacy Officer may be contacted at:

**City of Stockton Privacy Office**  
**Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street 3rd Floor, Stockton CA, 95202  
Telephone: 209-937-8233      Confidential fax #: 209-937-5702

## Your Protected Health Information

The term “**Protected Health Information**” (PHI) includes all information related to your past, present or future health condition(s) that individually identifies you or could reasonably be used to identify you and is transferred to another entity or maintained by the Plan in oral, written, electronic or any other form.

**PHI does not include** health information contained in employment records held by your employer in its role as an employer, including but not limited to health information on disability, work-related illness/injury, sick leave, Family or Medical Leave (FMLA), life insurance, dependent care flexible spending account, drug testing, etc.

## When the Plan May Disclose Your PHI

Under the law, the Plan may disclose your PHI without your written authorization in the following cases:

- **At your request.** If you request it, the Plan is required to give you access to your PHI in order to inspect it and copy it.
- **As required by an agency of the government.** The Secretary of the Department of Health and Human Services may require the disclosure of your PHI to investigate or determine the Plan’s compliance with the privacy regulations.
- **For treatment, payment or health care operations.** The Plan and its business associates will use your PHI (except psychotherapy notes in certain instances as described below) without your consent, authorization or opportunity to agree or object in order to carry out treatment, payment, or health care operations.

The Plan does not need your consent or authorization to release your PHI when you request it, a government agency requires it, or the Plan uses it for treatment, payment or health care operations.

The Plan Sponsor has **amended its Plan documents** to protect your PHI as required by Federal law. The Plan may disclose PHI to the Plan Sponsor for purposes of treatment, payment and health care operations in accordance with the Plan amendment. The Plan may disclose PHI to the Plan Sponsor for review of your appeal of a benefit or for other reasons related to the administration of the Plan.

<b>Definitions and Examples of Treatment, Payment and Health Care Operations</b>	
<b>Treatment</b> is health care.	Treatment is the provision, coordination or management of health care and related services. It also includes but is not limited to coordination of benefits with a third party and consultations and referrals between one or more of your health care providers. <ul style="list-style-type: none"> <li>• <b>For example:</b> The Plan discloses to a treating specialist the name of your treating primary care physician so the two can confer regarding your treatment plan.</li> </ul>
<b>Payment</b> is paying claims for health care and related activities.	Payment includes but is not limited to making payment for the provision of health care, determination of eligibility, claims management, and utilization review activities such as the assessment of medical necessity and appropriateness of care. <ul style="list-style-type: none"> <li>• <b>For example:</b> The Plan tells your doctor whether you are eligible for coverage or what percentage of the bill will be paid by the Plan. If we contract with third parties to help us with payment, such as a claims payer, we will disclose pertinent information to them. These third parties are known as “business associates.”</li> </ul>
<b>Health Care Operations</b> keep the Plan operating soundly.	Health care operations includes but is not limited to quality assessment and improvement, patient safety activities, business planning and development, reviewing competence or qualifications of health care professionals, underwriting, enrollment, premium rating and other insurance activities relating to creating or renewing insurance contracts. It also includes disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse compliance programs and general administrative activities. <ul style="list-style-type: none"> <li>• <b>For example:</b> The Plan uses information about your medical claims to refer you to a disease management program, to project future benefit costs or to audit the accuracy of its claims processing functions.</li> </ul>

## When the Disclosure of Your PHI Requires Your Written Authorization

Generally, the Plan will require that you sign a valid authorization form in order to use or disclose your PHI **other than:**

- When you request your own PHI
- A government agency requires it, or
- The Plan uses it for treatment, payment or health care operation.

You have the right to revoke an authorization.

Although the Plan does not routinely obtain psychotherapy notes, generally, an authorization will be required by the Plan before the Plan will use or disclose psychotherapy notes about you. Psychotherapy notes are separately filed notes about your conversations with your mental health professional during a counseling session. They do not include summary information

about your mental health treatment. However, the Plan may use and disclose such notes when needed by the Plan to defend itself against litigation filed by you.

The Plan generally will require an authorization form for uses and disclosure of your PHI for marketing purposes (meaning a communication that encourages you to purchase or use a product or service) if the Plan receives direct or indirect financial remuneration (payment) from the entity whose product or service is being marketed. The Plan generally will require an authorization form for the sale of protected health information if the Plan receives direct or indirect financial remuneration (payment) from the entity to whom the PHI is sold. The Plan does not intend to engage in fundraising activities.

## **Use or Disclosure of Your PHI Where You Will Be Given an Opportunity to Agree or Disagree Before the Use or Release**

Disclosure of your PHI to family members, other relatives and your close personal friends without your written consent or authorization is allowed if:

- The information is directly relevant to the family or friend's involvement with your care or payment for that care, and
- You have either agreed to the disclosure or have been given an opportunity to object and have not objected.

Under this Plan your PHI will automatically be disclosed to internal employer departments as outlined below. If you disagree with this automatic disclosure by the Plan you may contact the Privacy Officer to request that such disclosure not occur without your written authorization:

- In the event of your death while you are covered by this Plan, when the Plan is notified it will automatically communicate this information to the following internal departments: payroll, life insurance, deferred compensation.
- In the event the Plan is notified of a work-related illness or injury, the Plan will automatically communicate this information to the internal Workers' Compensation Coordinator and external Workers' Compensation provider to allow the processing of appropriate paperwork.
- In the event the Plan is notified of a condition that may initiate a long term disability benefit, the Plan will automatically communicate this information to the Long Term Disability (LTD) carrier to allow the processing of appropriate paperwork.
- In the event the Plan is notified of a situation where it may be possible to initiate a medical leave under the Family and Medical Leave Act (FMLA) benefit, the Plan will automatically communicate this information to the Human Resources Department FMLA Coordinator to allow the processing of appropriate FMLA paperwork.

**Note that PHI obtained by the Plan Sponsor's employees through Plan administration activities will NOT be used for employment related decisions.**

## **Use or Disclosure of Your PHI Where Consent, Authorization or Opportunity to Object Is Not Required**

In general, the Plan does not need your written authorization to release your PHI if required by law or for public health and safety purposes. The Plan and its Business Associates are allowed to use and disclose your PHI **without** your written authorization (in compliance with section 164.512) under the following circumstances:

1. When ***required by law***.
2. When permitted for ***purposes of public health activities***. This includes reporting product defects, permitting product recalls and conducting post-marketing surveillance. PHI may also be used or disclosed if you have been exposed to a communicable disease or are at risk of spreading a disease or condition, if authorized by law.
3. To a school about an individual who is a student or prospective student of the school if the protected health information this is disclosed is limited to ***proof of immunization***, the school is required by State or other law to have such proof of immunization prior to admitting the individual and the covered entity obtains and documents the agreements to this disclosure from either a parent, guardian or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or the individual, if the individual is an adult or emancipated.
4. When authorized by law to report information about ***abuse, neglect or domestic violence*** to public authorities if a reasonable belief exists that you may be a victim of abuse, neglect or domestic violence. In such case, the Plan will promptly inform you that such a disclosure has been or will be made unless that notice would cause a risk of serious harm. For the purpose of reporting child abuse or neglect, it is not necessary to inform the minor that such a disclosure has been or will be made. Disclosure may generally be made to the minor's parents or other representatives, although there may be circumstances under Federal or state law when the parents or other representatives may not be given access to the minor's PHI.
5. To a public health oversight agency for ***oversight activities authorized by law***. These activities include civil, administrative or criminal investigations, inspections, licensure or disciplinary actions (for example, to investigate complaints against

providers) and other activities necessary for appropriate oversight of government benefit programs (for example, to investigate Medicare or Medicaid fraud).

6. When required **for judicial or administrative proceedings**. For example, your PHI may be disclosed in response to a subpoena or discovery request, provided certain conditions are met, including that:
  - the requesting party must give the Plan satisfactory assurances a good faith attempt has been made to provide you with written Notice, and
  - the Notice provided sufficient information about the proceeding to permit you to raise an objection, and
  - no objections were raised or were resolved in favor of disclosure by the court or tribunal.
7. When required for **law enforcement health purposes** (for example, to report certain types of wounds).
8. For **law enforcement purposes** if the law enforcement official represents that the information is not intended to be used against the individual, the immediate law enforcement activity would be materially and adversely affected by waiting to obtain the individual's agreement and the Plan in its best judgment determines that disclosure is in the best interest of the individual. Law enforcement purposes include:
  - identifying or locating a suspect, fugitive, material witness or missing person, and
  - disclosing information about an individual who is or is suspected to be a victim of a crime.
9. When required to be given **to a coroner or medical examiner** to identify a deceased person, determine a cause of death or other authorized duties. When required to be given **to funeral directors** to carry out their duties with respect to the decedent; for use and disclosures for cadaveric **organ, eye or tissue donation** purposes.
10. For **research**, subject to certain conditions.
11. When, consistent with applicable law and standards of ethical conduct, the Plan in good faith believes the use or disclosure is necessary to prevent or lessen a serious and **imminent threat to the health or safety** of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.
12. When authorized by and to the extent necessary to comply with **workers' compensation** or other similar programs established by law.
13. When required, for **specialized government functions**, to military authorities under certain circumstances, or to authorized Federal officials for lawful intelligence, counter intelligence and other national security activities.

Any other Plan uses and disclosures not described in this Notice will be made only if you provide the Plan with written authorization, subject to your right to revoke your authorization, and information used and disclosed will be made in compliance with the minimum necessary standards of the regulation.

## Your Individual Privacy Rights

### A. You May Request Restrictions on PHI Uses and Disclosures

You may request the Plan to restrict the uses and disclosures of your PHI:

- To carry out treatment, payment or health care operations, or
- To family members, relatives, friends or other persons identified by you who are involved in your care.

The Plan, however, is not required to agree to your request if the Plan Administrator or Privacy Officer determines it to be unreasonable, for example, if it would interfere with the Plan's ability to pay a claim.

The Plan will accommodate an individual's reasonable request to receive communications of PHI by alternative means or at alternative locations where the request includes a statement that disclosure could endanger the individual. You or your personal representative will be required to complete a form to request restrictions on the uses and disclosures of your PHI. To make such a request contact the Privacy Officer at their address listed on the first page of this Notice.

### B. You May Inspect and Copy Your PHI

You have the right to inspect and obtain a copy (in hard copy or electronic form) of your PHI (except psychotherapy notes and information compiled in reasonable contemplation of an administrative action or proceeding) contained in a "designated record set," for as long as the Plan maintains the PHI. You may request your hard copy or electronic information in a format that is convenient for you, and the Plan will honor that request to the extent possible. You may also request a summary of your PHI.

A **Designated Record Set** includes your medical records and billing records that are maintained by or for a covered health care provider. Records include enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a health plan or other information used in whole or in part by or for the covered entity to

make decisions about you. Information used for quality control or peer review analyses and not used to make decisions about you is not included in the designated record set.

The Plan must provide the requested information within 30 days of its receipt of the request, if the information is maintained onsite or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if the Plan is unable to comply with the deadline and notifies you in writing in advance of the reasons for the delay and the date by which the Plan will provide the requested information.

You or your personal representative will be required to complete a form to request access to the PHI in your Designated Record Set. Requests for access to your PHI should be made to the Plan's Privacy Officer at their address listed on the first page of this Notice. You may be charged a reasonable cost-based fee for creating or copying the PHI or preparing a summary of your PHI.

If access is denied, you or your personal representative will be provided with a written denial describing the basis for the denial, a description of how you may exercise those review rights and a description of how you may complain to the Plan's Privacy Officer or the Secretary of the U.S. Department of Health and Human Services.

### ***C. You Have the Right to Amend Your PHI***

You or your Personal Representative have the right to request that the Plan amend your PHI or a record about you in a designated record set for as long as the PHI is maintained in the designated record set. The Plan has 60 days after receiving your request to act on it. The Plan is allowed a single 30-day extension if the Plan is unable to comply with the 60-day deadline (provided that the Plan notifies you in writing in advance of the reasons for the delay and the date by which the Plan will provide the requested information).

If the Plan denied your request in whole or part, the Plan must provide you with a written denial that explains the basis for the decision. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of your PHI. You should make your request to amend PHI to the Privacy Officer at their address listed on the first page of this Notice.

You or your personal representative may be required to complete a form to request amendment of your PHI. Forms are available from the Privacy Officer at their address listed on the first page of this Notice.

### ***D. You Have the Right to Receive an Accounting of the Plan's PHI Disclosures***

At your request, the Plan will also provide you with an accounting of disclosures by the Plan of your PHI during the six years (or shorter period if requested) before the date of your request. The Plan will not provide you with an accounting of disclosures related to treatment, payment, or health care operations, or disclosures made to you or authorized by you in writing. The Plan has 60 days after its receipt of your request to provide the accounting. The Plan is allowed an additional 30 days if the Plan gives you a written statement of the reasons for the delay and the date by which the accounting will be provided. If you request more than one accounting within a 12-month period, the Plan will charge a reasonable, cost-based fee for each subsequent accounting.

### ***E. You Have the Right to Request that PHI be Transmitted to You Confidentially***

The Plan will permit and accommodate your reasonable request to have PHI sent to you by alternative means or to an alternative location (such as mailing PHI to a different address or allowing you to personally pick up the PHI that would otherwise be mailed), if you provide a written request to the Plan that the disclosure of PHI to your usual location could endanger you. If you believe you have this situation, you should contact the Plan's Privacy Officer to discuss your request for confidential PHI transmission.

### ***F. You Have the Right to Receive a Paper or Electronic Copy of This Notice Upon Request***

To obtain a paper or electronic copy of this Notice, contact the Plan's Privacy Officer at their address listed on the first page of this Notice. This right applies even if you have agreed to receive the Notice electronically.

### ***G. Breach Notification***

If a breach of your unsecured protected health information occurs, the Plan will notify you.

## **Your Personal Representative**

You may exercise your rights to your protected health information (PHI) by designating a person to act as your Personal Representative. Your Personal Representative will generally be required to produce evidence (proof) of the authority to act on your behalf **before** the Personal Representative will be given access to your PHI or be allowed to take any action for you.

Under this Plan, proof of such authority will include (1) a completed, signed and approved Appoint a Personal Representative form; (2) a notarized power of attorney for health care purposes; (3) a court-appointed conservator or guardian; or, (4) for a Spouse under this Plan, the absence of a Revoke a Personal Representative form on file with the Privacy Officer.

**This Plan will automatically recognize your legal Spouse as your Personal Representative and vice versa, without you having to complete a form to Appoint a Personal Representative.** However, you may request that the Plan **not automatically** honor your legal Spouse as your Personal Representative by completing a form to Revoke a Personal Representative (copy attached to this notice or also available from the Privacy Officer).

**If you wish to revoke your Spouse as your Personal Representative, please complete the Revoke a Personal Representative form and return it to the Privacy Officer and this will mean that this Plan will NOT automatically recognize your Spouse as your Personal Representative and vice versa.**

The recognition of your Spouse as your Personal Representative (and vice versa) is for the use and disclosure of PHI under this Plan and is not intended to expand such designation beyond what is necessary for this Plan to comply with HIPAA privacy regulations.

You may obtain a form to Appoint a Personal Representative or Revoke a Personal Representative by contacting the Privacy Officer at their address listed on this Notice. The Plan retains discretion to deny access to your PHI to a Personal Representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect.

Because HIPAA regulations give adults certain rights and generally children age 18 and older are adults, if you have **dependent children age 18 and older** covered under the Plan, and the child wants you, as the parent(s), to be able to access their protected health information (PHI), that child will need to complete a form to Appoint a Personal Representative to designate you (the employee/retiree) and/or your Spouse as their Personal Representatives.

The Plan will consider a parent, guardian, or other person acting *in loco parentis* as the Personal Representative of an unemancipated minor (a child generally under age 18) unless the applicable law requires otherwise. **In loco parentis** may be further defined by state law, but in general it refers to a person who has been treated as a parent by the child and who has formed a meaningful parental relationship with the child for a substantial period of time. Spouses and unemancipated minors may, however, request that the Plan restrict PHI that goes to family members as described above under the section titled “Your Individual Privacy Rights.”

## **The Plan’s Duties**

The Plan is required by law to maintain the privacy of your PHI and to provide you and your eligible dependents with Notice of its legal duties and privacy practices. The Plan is required to comply with the terms of this Notice. However, the Plan reserves the right to change its privacy practices and the terms of this Notice and to apply the changes to any PHI maintained by the Plan. In addition, the Plan may not (and does not) use your genetic information that is PHI for underwriting purposes.

**Notice Distribution:** The Notice will be provided to each person when they initially enroll for benefits in the Plan (the Notice is provided in the Plan’s New Employee packets). The Notice is also available on the Plan’s website: [www.stocktongov.com](http://www.stocktongov.com). The Notice will also be provided upon request. Once every three years the Plan will notify the individuals then covered by the Plan where to obtain a copy of the Notice. This Plan will satisfy the requirements of the HIPAA regulation by providing the Notice to the named insured (covered employee) of the Plan; however, you are encouraged to share this Notice with other family members covered under the Plan.

**Notice Revisions:** If a privacy practice of this Plan is changed affecting this Notice, a revised version of this Notice will be provided to you and all participants covered by the Plan at the time of the change. Any revised version of the Notice will be distributed within 60 days of the effective date of a material change to the uses and disclosures of PHI, your individual rights, the duties of the Plan or other privacy practices stated in this Notice.

Material changes are changes to the uses and disclosures of PHI, an individual’s rights, the duties of the Plan or other privacy practices stated in the Privacy Notice. Because our health plan posts its Notice on its web site, we will prominently post the revised Notice on that web site by the effective date of the material change to the Notice. We will also provide the revised notice, or information about the material change and how to obtain the revised Notice, in our next annual mailing to individuals covered by the Plan.

## Disclosing Only the Minimum Necessary Protected Health Information

When using or disclosing PHI or when requesting PHI from another covered entity, the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply in the following situations:

- Disclosures to or requests by a health care provider for treatment,
- Uses or disclosures made to you,
- Disclosures made to the Secretary of the U.S. Department of Health and Human Services in accordance with their enforcement activities under HIPAA,
- Uses of disclosures required by law, and
- Uses of disclosures required for the Plan's compliance with the HIPAA privacy regulations.

This Notice does not apply to information that has been de-identified. **De-identified information** is information that does not identify you and there is no reasonable basis to believe that the information can be used to identify you.

As described in the amended Plan document, the Plan may share PHI with the Plan Sponsor for limited administrative purposes, such as determining claims and appeals, performing quality assurance functions and auditing and monitoring the Plan. The Plan shares the minimum information necessary to accomplish these purposes.

In addition, the Plan may use or disclose "summary health information" to the Plan Sponsor for obtaining premium bids or modifying, amending or terminating the group health Plan. **Summary health information** means information that summarizes claims history, claims expenses or type of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under a group health plan. Identifying information will be deleted from summary health information, in accordance with HIPAA.

## Your Right to File a Complaint

**If you believe that your privacy rights have been violated, you may file a complaint with the Plan in care of the Plan's Privacy Officer, at the address listed on the first page of this Notice.** Neither your employer nor the Plan will retaliate against you for filing a complaint.

You may also file a complaint (within 180 days of the date you know or should have known about an act or omission) with the Secretary of the U.S. Department of Health and Human Services by contacting their nearest office as listed in your telephone directory or at this website (<http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html>) or this website: <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html> or contact the Privacy Officer (noted on the first page) for more information about how to file a complaint.

## If You Need More Information

If you have any questions regarding this Notice or the subjects addressed in it, you may contact the Plan's Privacy Officer at the address listed on the first page of this Notice.

*See attached form to Revoke a Personal Representative, if needed.*

**CITY OF STOCKTON**  
**Form to Revoke a Personal Representative**

---

Complete the following chart to indicate the name of the Personal Representative to be revoked:

	Plan Participant	Person to be Revoked as my Personal Representative
<b>Name (print):</b>		
<b>Address (City, State, Zip):</b>		
<b>Phone:</b>	(    )	(    )

I, \_\_\_\_\_ (*Name of Participant or Beneficiary*)  
 hereby revoke the authority of \_\_\_\_\_ (*Name of Personal Representative*)

to act on my behalf,

to act on behalf of my dependent child(ren), named:

\_\_\_\_\_,  
 in receiving any protected health information (PHI) that is (or would be) provided to a personal representative,  
 including any individual rights regarding PHI under HIPAA, effective \_\_\_\_\_,  
 20\_\_\_\_.

I understand that PHI has or may already have been disclosed to the above named Personal Representative prior to  
 the effective date of this form.

\_\_\_\_\_  
 Participant or Beneficiary's Signature

\_\_\_\_\_  
 Date

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
 400 E. Main Street 3rd Floor, Stockton CA, 95202  
 Telephone: 209-937-8233      Confidential fax #: 209-937-5702

## SAMPLE HIPAA PRIVACY NOTICE COVER MEMO

Dear Plan Participant:

Under a Federal law called the Health Insurance Portability and Accountability Act (HIPAA), group health plans across the nation, including the City of Stockton group health plan, must create a Notice of Privacy Practice and provide you with a copy.

Attached is our Plan's Notice of Privacy Practice. You should review it and keep it for future reference. Please take a moment to note the following important information in the attached document.

1. Please share this Notice of Privacy Practice with other plan participants in your household.
2. This Privacy Notice will tell you about your rights and our Plan's obligations concerning your protected health information.
3. Note the address of the Plan's Privacy Officer that appears on page 1.
4. Please review the information on page 5 about Personal Representatives and how this Plan will recognize your designated Personal Representative and how our City Human Resources Department will work with you and your spouse on sharing health information with one another.
5. If you have children over age 18 covered under our Plan, you will want to review the Personal Representative section as mentioned above, to see how we will share their information with you.
6. You may also receive similar Notices of Privacy Practices from insured group health plans in which you are enrolled.

We hope you find the enclosed information helpful. We take responsibility to protect the health information our group health plan obtains and to safeguard information that you share with our group health plan.

For questions about this notice, contact the City of Stockton Human Resources Department at (209) 937-8233.

Sincerely,

The City of Stockton

## SAMPLE COMBINED HIPAA PRIVACY AND WHCRA NOTICE

### Annual Notice: Women's Health and Cancer Rights Act (WHCRA)

If you have had or are going to have a mastectomy, you may be entitled to certain benefits under the Women's Health and Cancer Rights Act of 1998 (WHCRA). For individuals receiving mastectomy-related benefits, coverage will be provided in a manner determined in consultation with the attending physician and the patient, for:

- All stages of reconstruction of the breast on which the mastectomy was performed;
- Surgery and reconstruction of the other breast to produce a symmetrical appearance;
- Prostheses; and
- Treatment of physical complications of the mastectomy, including lymphedema.

These benefits will be provided subject to the same deductibles, copayment and coinsurance applicable to other medical and surgical benefits provided under the Medical Plan. If you would like more information on WHCRA benefits, please contact the City of Stockton Human Resources Department at (209) 937-8233.

---

---

### Where to Find a HIPAA Privacy Notice for Our Group Health Plan

HIPAA Privacy pertains to the following group health plan benefits sponsored by the City of Stockton:

- self-funded medical plan options including outpatient prescription drug benefits and health reimbursement account (HRA),
- self-funded dental plan,
- self-funded vision plan,
- Independent Review Organizations for External Reviews,
- COBRA administration, and
- Health Flexible Spending Account (FSA) administration

You are provided with a complete HIPAA Privacy Notice when you enroll for these benefits. You can obtain another copy of the plan's HIPAA Privacy Notice by going to the Intranet site at <http://cosintranet.ci.stockton.ca.us> or you can write or call the City of Stockton Human Resources Department at 400 E. Main Street, 3<sup>rd</sup> Floor Stockton, CA 95202, or call (209) 937-8233

HIPAA Privacy Notices that pertain to the insured medical and dental benefits can be obtained by contacting the City of Stockton's Human Resources Department at (209) 937-8233.

## HIPAA PRIVACY POLICY AND PROCEDURE ON THE PRIVACY OFFICER

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(a) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

- The Plan must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the Plan. The Plan must document the personnel designation.
- The Plan must designate a contact person or office who is responsible for receiving complaints about the Privacy policies and procedures of this Plan and who is able to provide further information about matters covered by the required HIPAA Privacy Notice. The Plan must document the personnel designation.

### KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

### PROCEDURES

1. Under this Plan, the Privacy Officer is the City's **Deputy Director of Human Resources –Rick and Benefits** and is also the person who will receive complaints about the Privacy policies and procedures of this Plan as noted above.
2. In the absence of the Privacy Officer (such as for sickness or vacation) the following person(s) become the designee of the Privacy Officer under this Plan. The first designee will assume the duties of the Privacy Officer in the absence of the Privacy Officer. In the absence of the first designee, the second designee will assume the duties, and so forth.
  - **First Designee:** the City of Stockton Supervising Human Resource Analyst - Benefits
  - **Second Designee:** Human Resources Analyst - Benefits
3. Questions regarding the HIPAA privacy notice will be answered by the Privacy Officer or their designee.
4. The Privacy Officer will follow the job description associated with this position and will oversee the Plan's Privacy compliance operations, policies and procedures.
5. The Privacy Officer and their designees have undergone or will undergo a background check to help assure that these individuals are appropriate to access PHI. The background check will include, as part of the plan's clearance procedures, the following:
  - Written application for employment.
  - Written proof of citizenship or resident alien status.
  - Confirmation of prior employment history.
  - Request professional/personal references and contact those references.
  - Confirm educational history and practicing credentials.
  - Verification of any relevant license(s).
  - Conduct a criminal background check (using a background check service).
  - Verification of Social Security Number.

Information of concern will be reviewed with the plan's legal counsel.

6. The Privacy Officer will use the resources listed below in order to answer questions and implement the Policies and Procedures.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR Section 164.530(a)
- The Plan's Privacy Officer
- City of Stockton attorney's office at 425 N. El Dorado St, 2<sup>nd</sup> floor Stockton, CA 95202 or call (209) 937-8333.

## Position Description for the Privacy Officer for the City of Stockton

---

---

**Position Title:** Privacy Officer

**Immediate Supervisor:** Director of Human Resources, City of Stockton

**General Purpose:** The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the Plan's policies and procedures covering the privacy of, and access to, protected health information in compliance with Federal and state laws and the Plan's information privacy practices. The "Plan" refers to the group health plan as defined on the cover page of the Plan's HIPAA Privacy Policy and Procedure Manual.

**Responsibilities:**

- Coordinates the development and updating of the Plan's HIPAA Privacy policies and procedures
- Oversees that Plan staff adhere to the Plan's HIPAA privacy policies and procedures.
- Works with the group health plan benefits administration staff of the Human Resources Department and the Information Technology (IT) Department/staff to establish necessary operational steps needed for the Plan to comply with the Federal HIPAA regulations, such as the use of authorization forms, verification of identify, use of personal representative forms, safety of electronic PHI, etc.
- Performs initial privacy risk assessments to see where the Plan needs to enhance their compliance with HIPAA privacy regulations.
- Coordinates and/or conducts ongoing HIPAA Privacy compliance monitoring activities to assure continued compliance with the HIPAA regulations.
- Serves as the designated decision-maker for issues and questions involving interpretation of the privacy policies and procedures and the applicability of the HIPAA privacy rules to the Plan, (in coordination with legal counsel, as appropriate). Initiates, facilitates, and promotes activities to foster privacy information awareness within the Plan.
- Ensures that where appropriate Plan documents are amended in order to comply with HIPAA Privacy.
- Identifies all Business Associates and assures that the Plan maintains signed business associate contracts with all applicable parties. Routes business associate contracts received by the Plan to legal counsel for review.
- Publishes and distributes the HIPAA privacy notice.
- Investigates all Privacy complaints with corrective action as appropriate. Investigate any potential privacy breach incidents, including performing risk assessments and if necessary, managing the provision of notices to individual affected by a breach and notice to HHS as required. Works with legal counsel on complaints/breach incidents as appropriate.
- Oversees the process on sanctioning of employees that violate a Plan HIPAA privacy policy/procedure.
- Oversees, directs, delivers, or ensures delivery of HIPAA privacy training and orientation to all employees, volunteers, IT Department staff, and when applicable, to business associates and other appropriate third parties.
- Establishes structures to ensure an individual's rights, as guaranteed under HIPAA, such as the right to amend and to restrict access to protected health information when appropriate. Establishes a mechanism to track access to protected health information, within the purview of the Plan and as required by law, in order to allow qualified individuals to review or receive a report on such activity.
- Ensures compliance with privacy practices and where necessary, the consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with the City's Human Resources Department, the Plan's HIPAA Security officer, administration and legal counsel as applicable.

- Serves as the information privacy liaison for users of any group health plan systems (both paper and electronic).
- Oversees the development and implementation of appropriate firewalls between the employer organization and the group health Plan.
- Works with all group health plan staff involved with the release of protected health information, to ensure coordination and cooperation with HIPAA regulations and the Plan's policies and procedures.
- Tracks the release of PHI that is not for purposes of treatment, payment or operations so that individuals may review or receive a report on such activities.
- Maintains current knowledge of applicable Federal and state privacy laws and updates the Plan's compliance as needed.
- Cooperates with the Office of Civil Rights or other applicable government agencies, or external auditors in any compliance reviews or investigations.

**Qualifications:**

- Education and experience relative to the size and scope of the organization.
- Demonstrated organization, facilitation, communication and presentation skills.
- Knowledge and experience in information privacy laws such as HIPAA.
- Knowledge in and the ability to apply the principles of health information management, project management, and change management.
- Obtains and successfully passes a background check to help assure that this individual is appropriate to access PHI. The background check is part of the plan's clearance procedures.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR AUTHORIZATIONS

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.508 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. Except as otherwise provided under the privacy regulations or other applicable law, the Plan may not use or disclose PHI without a valid authorization.
2. An authorization is not required for use or disclosure of PHI for treatment, payment or health care operations or for uses or disclosures otherwise permitted under the privacy rules.
3. When the Plan obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure will be consistent with such authorization.
4. **Authorization for Psychotherapy notes:** Notwithstanding any other provision of the regulations, the Plan will obtain an authorization for any use or disclosure of psychotherapy notes, except:
  - To carry out treatment, payment, or health care operations; or
  - Use or disclosure by the Plan to defend itself in a legal action or other proceeding brought by the individual; and as otherwise permitted under the regulations.
5. **Authorization for Marketing:** Notwithstanding any provision of the regulations, the Plan will obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of a face-to-face communication made by a covered entity (group health plan or health care provider) to an individual or a promotional gift of nominal value provided by the Plan. See the definition of Marketing in this policy.

If the marketing involves direct or indirect financial remuneration to the Plan from a third party, the authorization will state such remuneration is involved.

**Authorization Required For Sale of Protected Health Information:** A covered entity (the Plan) must obtain an authorization for any disclosure of protected health information that is a sale of protected health information. Such authorization must state that the disclosure will result in remuneration to the covered entity (the Plan).

6. **Valid Authorization:** A valid authorization is a document that meets the requirements of the regulations and contains the **Core Elements** (as noted below). A valid authorization may contain elements or information in addition to the elements required by the regulation, provided that such additional elements or information are not inconsistent with the elements required by the regulations.

**Core elements and required statements:** A valid authorization must contain at least the following **core elements**:

- a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- c. The name or other specific identification of the person(s), or class of persons, to whom the Plan may make the requested use or disclosure;
- d. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. [The statement "end of research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.]
- f. Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

**A valid authorization must contain the required statements** adequate to place the individual on notice of all of the following:

- a. The individual's right to revoke the authorization in writing, and a description of how the individual may revoke the authorization or reference to the Plan's HIPAA Privacy Notice where such information is to be provided.
- b. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either
  - the Plan may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization **or**
  - (consistent with the regulations) the consequences to the individual of refusal to sign the authorization when the Plan can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

The potential for information disclosed pursuant to the authorization to be subject to **redisclosure** by the recipient and no longer be protected by the Privacy regulations.

**An authorization is not valid, if the document submitted has any of the following defects:**

- a. The expiration date has passed or the expiration event is known by the Plan to have occurred;
  - b. The authorization has not been filled out completely,
  - c. The authorization is known by the Plan to have been revoked;
  - d. The authorization violates paragraph (b)(3) of section 164.508 of the regulation (meaning the authorization violates what is permitted as a compound authorization as described in #7 below) or the authorization violates paragraph (b)(4) of section 164.508 of the regulation (meaning the Plan is not permitted to require that an authorization be signed for treatment, payment and health care operations) if applicable;
  - e. Any material information in the authorization is known by the Plan to be false.
7. **Compound authorizations:** An authorization for use or disclosure of protected health information (PHI) may not be combined with any other document to create a compound authorization, **except as follows:**
- a. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study, including another authorization for the use or disclosure of PHI for such research.

This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research related treatment on the provision of one of the authorizations, of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.
  - b. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.
  - c. An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other authorization, **except** a covered entity may NOT condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.
8. **Prohibition on conditioning of authorizations:** The Plan will not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:
- a. The Plan may condition the enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, **if:**
    - The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
    - The authorization is not for a use or disclosure of psychotherapy notes; and
  - b. The Plan may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

9. The Plan will create authorizations that are written in plain language.
10. If the Plan seeks an authorization from an individual for a use or disclosure of PHI, the Plan will provide the individual with a copy of the signed authorization.
11. **Revoking an authorization:** An individual may revoke an authorization at any time, provided that the revocation is in writing to the Plan, except to the extent that the Plan has already taken action.
12. The Plan will document and retain signed authorizations consistent with the regulations (6 years from the later of the date the authorization was created or the last day the authorization was in effect).

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

**Authorization** refers to a valid authorization as described in the policy above.

**Marketing** means (according to 164.501), to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

- i. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
- ii. For the treatment of the individual; or
- iii. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

An arrangement between the Plan and any other entity whereby the Plan discloses PHI to the other entity, in exchange for direct or indirect financial remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

## PROCEDURES

- 1) A valid authorization is required for any use or disclosure of PHI, except as provided under these procedures or under the privacy regulations.
- 2) An **authorization is not required** for use or disclosure of PHI for treatment, payment or health care operations or disclosure of a person's own PHI to that same person. The Plan will not obtain authorization when it makes the following disclosures to the Plan Sponsor.
  - a. Summary health information in which the 18 individual identifiers have been removed. (See the Policy/procedure on De-identification for a list of the 18 identifiers.)
  - b. For Plan administration and payment functions such as claim appeals as long as the Plan Sponsor de-identifies claim appeals presented for decision-making. Where the claimant needs to be identified, the claimant will be asked to sign an authorization form.
- 3) The **Plan will seek authorization** for the following uses and disclosure of PHI:
  - a. **To a third party** (other than the Plan's business associate with whom the Plan has a signed BA agreement) for the purpose of assisting an individual with a claim issue or other health benefits issue that necessitates PHI.
  - b. To use or disclosure PHI related to an individual's attendance at a claim review meeting for the purpose of evaluating the individual's claim appeal.
  - c. **When the Plan is unsure if the Plan is permitted to release PHI without an authorization.**
  - d. **For marketing purposes.** Refer to the Plan's marketing policy and procedure for more information.
  - e. **For sale of PHI.** The authorization must state if the disclosure will result in remuneration to the covered entity
  - f. **For PHI related to a deceased individual (as executed by their personal representative), unless the individual has been deceased for more than 50 years.**

- g. **For the use or disclosure of psychotherapy notes** except:
- Use or disclosure by the Plan to defend a legal action;
  - For use or disclosure to the Secretary of Health and Human Services (HHS) regarding compliance;
  - Use or disclosure as required by law;
  - Use or disclosure for health oversight activities with respect to the oversight of the originator of the notes;
  - Use or disclosure to coroners, medical examiners and funeral directors; or
  - Use or disclosure to avert a serious threat to health or safety.
- 4) If the Plan seeks an authorization for a use or disclosure of PHI, the Plan must provide the individual with a copy of the signed authorization.
  - 5) The Privacy Officer will make a determination as to whether a specific use or disclosure of PHI requires an authorization.
  - 6) If the Privacy Officer determines that an authorization is required, then the Plan will attempt to obtain a valid authorization from the individual.
  - 7) The Plan will use the Plan-approved authorization form (in this manual) that has been determined to be a valid authorization form. The Plan's Authorization has been drafted for a plan that is not subject to more stringent state medical privacy laws.
    - If the Plan uses an authorization form **for marketing purposes where the Plan is receiving financial remuneration (payment)** from the third party whose service or item is being marketed, the Plan will revise the marketing statement on the authorization form to disclose that the Plan is receiving payment from a third party.
    - If the Plan uses an authorization form **for purposes of the sale of protected health information, where the Plan is receiving financial remuneration (payment)**, the Plan will revise the sale of protected health information statement on the authorization form to disclose that the Plan is receiving payment from the sale of PHI.
  - 8) When the authorization form is completed and sent back to the Plan by a covered individual, the Privacy Officer or designee will review the form to ensure that it is signed and complete.
  - 9) If the form has not been signed, is not properly completed or is otherwise defective, the Privacy Officer will resend the form to the covered individual with a specific explanation of the reason for rejecting the form.
  - 10) The authorization must have an expiration date and must be signed and dated. An authorization is not valid if:
    - The expiration date has passed or the expiration event is known by the Privacy Officer to have occurred.
    - The authorization has not been filled out completely.
    - The authorization is known by the Privacy Officer to have been revoked.
    - Any material information in the authorization is known by the Privacy Officer to be false.
  - 11) Authorizations should be on separate forms. If two authorizations are required, separate forms should be used. The Plan understands that an authorization for use or disclosure of protected health information (PHI) may not be combined with any other document to create a compound authorization, except as outlined in item "7" in the policy section of this policy/procedure.
  - 12) The Plan will generally not condition the provision of treatment, payment, enrollment or eligibility on receipt of an authorization from the individual.
  - 13) If a personal representative signs the authorization form, then there must be proof of the representative's authority on file with the Plan in the City's Human Resources Office.
  - 14) An individual may revoke an authorization at any time by providing a signed request to the Privacy Officer by mail, email, facsimile or hand-delivery.
    - A verbal revocation will not be valid.
    - A revocation will not be valid to the extent the Plan has already relied on the authorization.
  - 15) The Privacy Officer will retain signed authorizations consistent with the HIPAA regulations and in accordance with this Plan's Record Retention Policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.508.
- The Plan's Privacy Officer.

**City of Stockton**  
**Authorization Form for Release of Personal Health Information (PHI)**

---

---

I, \_\_\_\_\_, hereby authorize the use or disclosure of the health information as described in this authorization.

1. Specific person/organization/or class of persons authorized to **provide** the information:  
\_\_\_\_\_
2. Specific person/organization/or class of persons authorized to **receive** and use the information (*insert name, title, address fax, phone and e-mail if possible*):  
\_\_\_\_\_
3. Specific **description of the information to be used or disclosed** (*Include names of individuals to whom the information pertains such as a minor child, description of information and dates, as appropriate*):  
\_\_\_\_\_
4. **Purpose of the request:** (*Check one*)     At the request of the individual signing this form.  
 Other: \_\_\_\_\_
5. **Right to Revoke:** I understand that this authorization is voluntary and that I have the right to revoke this authorization at any time by notifying the Privacy Officer (in writing) at the address noted in the box at the bottom of this form. I understand that such a revocation is only effective after it is received and logged by the Privacy Officer. I understand that any use or disclosure made prior to the revocation of this authorization will not be affected by a revocation.
6. **I understand that after this information is disclosed, Federal law might not protect it and the recipient might disclose it again.**
7. I understand that I am entitled to receive a copy of this authorization and the information described on this form if I ask for it.
8. I understand that this authorization will expire as indicated here:     One year from the date of this authorization.  
 On the following date: \_\_\_\_\_, 20\_\_.
9. The Plan will not condition treatment, payment, enrollment or eligibility for benefits on receipt of an authorization.
10. If this authorization is **for marketing purposes**, this Plan is not receiving financial remuneration (payment) from the third party whose service or item is being marketed. If the authorization is **for the sale of protected health information**, the disclosure will not result in remuneration (payment) to the Plan.

---

\_\_\_\_\_  
Signature of Individual

\_\_\_\_\_  
Date

or

---

\_\_\_\_\_  
Signature of Personal Representative

\_\_\_\_\_  
Date

If a Personal Representative executes this form, that Representative warrants that he or she has authority to sign the authorization form on the basis of:  a signed Personal Representative Form; or  Other \_\_\_\_\_

---

---

Acknowledgement by the Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_, 20\_\_

*This authorization reflects the requirements of 45 CFR § 164.508 (8-14-02) and updated for HIPAA Omnibus (9-23-13).*

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street, 3<sup>rd</sup> Floor    Stockton CA, 95202  
Telephone: 209-937-8233    Confidential fax #: 209-937-5702



## HIPAA PRIVACY POLICY AND PROCEDURE FOR PERSONAL REPRESENTATIVES

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502 (g) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

**The Plan will provide relevant protected health information (PHI) to personal representatives of an individual, unless, the Plan is otherwise prevented by law from doing so.**

- A. **Individuals:** The Plan must treat a personal representative as the “individual” for purposes of the HIPAA privacy rules. Therefore the Plan must provide PHI about an individual only to and about that individual unless the law permits otherwise (such as the release of PHI for treatment payment and health care operation or with a signed authorization form or where an individual has formally elected a personal representative).
- B. **Employee and Spouse:** Under this Plan, and as stated in the Plan’s HIPAA Privacy Notice, **this Plan will automatically honor an employee’s spouse as the employee’s personal representative and vice versa unless that employee and/or spouse do not want this provision to be followed in which case the employee and/or spouse may request, from the Plan’s Privacy Officer, that such personal representation not be automatically honored. The individual will be requested to complete a form to “Revoke a Personal Representative.”** In this case the Plan will follow the procedures described below under the procedure’s section for personal representative.

Per section 164.510(b)(3) of the regulation, the Plan may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. This rule extends to the PHI of a deceased individual unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the Plan.

- C. **Adults and Emancipated Minors:** If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, the Plan must treat such person as a personal representative with respect to PHI. Note that a power of attorney that does not include decisions related to health care in its scope would not be sufficient to create personal representative status for purposes of the HIPAA privacy rules. Thus, a person with an individual's power of attorney may or may not be the individual's personal representative for HIPAA privacy purposes, depending on whether the power of attorney includes authority to act on behalf of the individual in decisions related to health care.
- D. **Unemancipated Minors:** If under applicable law a parent, guardian or other person acting “in loco parentis” (in place of the parent) has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the Plan must treat such person as a personal representative with respect to PHI. However, such person may not be a personal representative of an unemancipated minor and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service if:
- The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
  - The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or
  - A parent, guardian, or other person acting *in loco parentis* assents (agrees) to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

Notwithstanding the provisions of the above text regarding unemancipated minors:

- As permitted by law, the Plan may disclose (or not disclose) PHI or provide access (or no access) to PHI about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis* in accordance with the Plan’s policy and procedure on “Access of Individuals to PHI.”
- Where the parent, guardian, or other person acting *in loco parentis*, is **not** the personal representative (as described above in this policy) and as permitted by law the Plan may provide or deny access under to a parent, guardian, or other

person acting *in loco parentis*, (in accordance with the Plan's policy on "Access of Individuals to PHI) provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

- E. **Deceased individuals:** If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Plan must treat such person as a personal representative with respect to PHI relevant to such personal representation.

The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the privacy rules.

- F. **Abuse, neglect, endangerment situations:** As permitted by law, the Plan may elect **not** to treat a person as the personal representative of an individual if the Plan has a reasonable belief that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- Treating such person as the personal representative could endanger the individual; and
- The Plan, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

**Emancipated Minor:** Generally emancipated minors are under eighteen, not married, not serving in the armed forces, self-supporting for two years, not living with parents and have completely severed the parental relationship as to all legal rights and liabilities, including care, custody, control and service for two years.

The Plan should consult legal advice in situations where a minor wants to act as their own personal representative.

Emancipation is not available in every state in the United States. Where it is available, emancipation is a legal process by which minors can attain legal adulthood before reaching the age at which they would normally be considered adults (this is called the "age of majority"). The rights granted to legally emancipated minors might include the ability to sign legally binding contracts, own property, and keep one's own earning. However, each state has different laws governing emancipation and some states simply have no law or legal process concerning emancipation. In states where minors wish to become legally emancipated they will have to break new legal ground. Married minors are typically considered to be emancipated minors.

**Individual** means the person who is the subject of protected health information.

**Family Member** means, with respect to an individual:

1. A dependent (as such term is defined in 45 CFR 144.103, which says "any individual who is or may become eligible for coverage under the terms of a group health plan because of a relationship to a participant"), of the individual; or
2. Any other person who is a first-degree, second-degree, third-degree, or fourth degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
  - a. First-degree relatives include parents, spouses, siblings, and children.
  - b. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
  - c. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
  - d. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

**Personal Representative** is not specifically defined by the HIPAA regulations. For this Plan it means any adult who has the authority by law or by written agreement from the individual, to act in place of that individual.

## PROCEDURES

1. **Recognition of Personal Representative:** Other than those individuals deemed to be personal representatives as described in this Policy and the Plan's Notice of Privacy Practice, the Plan will only treat an individual as a personal representative where:
  - a personal representative form has been completed and signed;
  - the Plan office has received a notarized power of attorney for health care purposes document; or
  - the Plan office has received a court-appointed conservator or guardian document.

- a. The parents or guardians of an unemancipated minor who have authority to act on the minor's behalf in making decisions relating to health care generally are the personal representatives of the minor with respect to the PHI related to that health care. However, there are exceptions to this rule, and even if the parent is not the minor's personal representative, the parent may still have access to the minor's PHI under certain circumstances.
  - b. An individual's spouse generally is not automatically the individual's personal representative for purposes of the HIPAA privacy rules simply by virtue of the marriage. However under this Plan, and as explained in our Plan's Notice of Privacy Practice, we honor the employee's spouse as their personal representative for Plan benefit payment-type purposes and vice versa, and allow an individual to revoke a spouse as their personal representative, as desired by completing a "Form to Revoke a Personal Representative".
  - c. The Plan may disclose to a family member (as defined in this policy/procedure), other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Plan will treat such person as a personal representative with respect to PHI of the deceased person.
  - d. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the privacy rules.
2. **Designation of Personal Representative:** This Plan will use a written form, called "Form to Appoint a Personal Representative" to record information about personal representatives. The form is available from the Privacy Officer, Human Resources Department or the benefits website. HR Department posts forms to the website.
  3. **Revoke A Personal Representative:** The Plan allows a person to revoke a previously designated personal representative by completing a form called "Revoke a Personal Representative" available from the Privacy Officer, Human Resources Department or the benefits website. HR Department posts forms to the website.
  4. **Designate a New Personal Representative:** To designate another individual as personal representative, a new personal representative form must be completed and approved by the Plan.
  5. **Verification of Personal Representatives:** All personal representatives will be subject to the Plan's verification procedure (see the policy and procedure on "Verification of Identity.")
  6. **Duration of Effectiveness of a Personal Representative:** Where a personal representative form has been completed and approved, it will be recognized by the Plan as long as the individual making the designation is covered by the Plan or until the form is revoked.
  7. **Records:** The Plan will maintain personal representative designation and revocation forms in compliance with the Plan's policy and procedure on "Record Retention and Destruction."

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.502 (g).
- The Plan's Privacy Officer.
- <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html>

CITY OF STOCKTON

Form to Appoint a Personal Representative

Complete the following chart to indicate the name of the proposed Personal Representative

Table with 3 columns: Plan Participant, Proposed Personal Representative, and fields for Name, Address, and Phone. Includes an important note about inserting the Personal Representative's Password for Telephonic Identification.

I, \_\_\_\_\_ [Name of Participant or Beneficiary] hereby designate \_\_\_\_\_ [Name of Personal Representative]:

- to act on my behalf,
to act on behalf of my dependent child(ren) named:

in receiving:

- any protected health information (PHI) that is (or would be) provided to me as a participant/beneficiary of the Plan, including any individual rights that I have regarding my PHI under HIPAA.
only the following protected health information to conduct the following functions on my behalf:

I understand that this designation of a Personal Representative is subject to approval by the Plan. I also understand that, once approved, this designation will remain in effect unless I revoke it. I understand that I have the right to revoke this designation at any time by completing a form to Revoke a Personal Representative available from the Privacy Officer. I understand that I may review a copy of the Plan's Policy on Personal Representatives.

Participant or Beneficiary's Signature Date

Personal Representative's Signature Date

The above Personal Representative request is:

- approved.
not approved because:

Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_

Once completed, please return this form to the:
City of Stockton Deputy Director of Human Resources - Risk & Benefits
400 E. Main Street, 3rd Floor Stockton CA, 95202
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

**CITY OF STOCKTON**  
**Form to Revoke a Personal Representative**

---

Complete the following chart to indicate the name of the Personal Representative to be revoked:

	Plan Participant	Person to be Revoked as my Personal Representative
<b>Name (print):</b>		
<b>Address (City, State, Zip):</b>		
<b>Phone:</b>	(    )	(    )

I, \_\_\_\_\_ (*Name of Participant or Beneficiary*)  
 hereby revoke the authority of \_\_\_\_\_ (*Name of Personal Representative*)

to act on my behalf,

to act on behalf of my dependent child(ren), named:

\_\_\_\_\_,  
 in receiving any protected health information (PHI) that is (or would be) provided to a personal representative,  
 including any individual rights regarding PHI under HIPAA, effective \_\_\_\_\_, 20\_\_\_\_.

I understand that PHI has or may already have been disclosed to the above named Personal Representative prior to  
 the effective date of this form.

\_\_\_\_\_  
 Participant or Beneficiary's Signature

\_\_\_\_\_  
 Date

Acknowledgement by the Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_, 20\_\_\_\_

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
 400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
 Telephone: 209-937-8233 Confidential fax #: 209-937-5702

## HIPAA PRIVACY POLICY AND PROCEDURE FOR MINIMUM NECESSARY

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502 (b) and 514 (d) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

- A. When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, the Plan or business associate will make reasonable efforts to limit PHI to the **minimum necessary to accomplish the intended purpose of the use, disclosure or request**.
- B. The Plan has implemented these policies and procedures for routine uses and disclosures. **This minimum necessary policy applies to oral, electronic, and written PHI.**

**Minimum necessary standard does not apply to the following uses and disclosures:**

- for requests by a health care provider for treatment;
- to the individual;
- made in accordance with a valid authorization;
- made to the Secretary of the Department of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated;
- for which an authorization or opportunity to agree or disagree is not required under the regulation;
- that are required for compliance with the general rules under §164.502; and
- required for compliance with HIPAA electronic data interchange (EDI) transaction standards.

- C. In order to comply with the **minimum necessary requirements** the Plan will:

1. Identify those persons or classes of persons, as appropriate, in the **workforce who need access** to PHI to carry out their duties;
  - Identify the categories of PHI to which access is needed and the conditions appropriate to such access.
  - Make reasonable efforts to limit the access of its workforce as described above.
2. Disclose protected health information, as follows:
  - For routine disclosures made on a recurring basis, the Plan will establish procedures **that limit PHI to the amount reasonably necessary to achieve the purpose** of the disclosure;
  - For other disclosures the Plan will **develop and use criteria** designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose of the disclosure; and
  - Review non-routine requests for disclosure on an individual basis.
  - To the extent practicable, the Plan will only use, disclose or request **limited data set** information. This limited data set information excludes the following direct identifiers of the individual or their relatives, employers or household members:
    1. Names
    2. Postal address information except town, city, state and zipcode
    3. Telephone and fax numbers
    4. Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers or certificate/license numbers
    5. Vehicle identifiers and serial numbers including license plate numbers, and device identifiers and serial numbers
    6. Email addresses, web universal resource locators (URLs), and internet protocol (IP) address numbers and
    7. Biometric identifiers such as finger and voice prints, full face photographic images and any comparable images.

Limited data set information may include dates related to the individual such as birth date or dates of admission or discharge, and certain geographic information such as an individual's town, city, state or zipcode.

3. Rely upon a requested disclosure as being the minimum necessary for the stated purpose, when the information is requested by one of the following and the requestor represents that the information is the minimum necessary for the stated purpose.
  - public officials that are permitted under 164.512 (see this Plan's policy on "Disclosure of PHI for Public Health, etc.");
  - another covered entity;
  - a professional who is a member of the Plan's workforce or is a **business associate** of the Plan for the purpose of providing professional services to the Plan; or
  - documentation or representations that comply with the applicable requirements related to research.
4. Request information from another covered entity that is:
  - Limited to that which is reasonably necessary to accomplish the purpose of the request;
  - For routine, recurring basis, in accordance with the Plan's standard procedures; or
  - For other requests, in accordance with specific criteria. Such requests will be reviewed on an individual basis.
5. The Plan will not request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the use, disclosure, or request.

#### D. Disclosures to Business Associates.

- i. A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
- ii. A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with your Business Associate agreement, that the subcontractor will appropriately safeguard the information.

The satisfactory assurances required by disclosures to business associates must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of your Business Associate agreement.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

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

## PROCEDURES

1. The Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when:
  - (a) using PHI internally,
  - (b) disclosing PHI to an external party in response to a request, and
  - (c) requesting PHI from another covered entity or a business associate.
2. The Plan understands that when it shares PHI with a contracted business associate, that business associate may disclose PHI to a business associate that is a subcontractor of that business associate, provided there is a business associate contract between the subcontractor and the business associate.

3. Employees have been divided into categories of permission (or accessibility) to PHI as noted in the chart below. The Plan’s data security measures designed to protect PHI and limit access to PHI corresponds to the following chart. The Plan has identified those individuals who need access to PHI to carry out their daily job duties. Employees are identified in the chart below.

Employees with Full Access to PHI	Employees with Limited Access to PHI	Employees with Full Access to PHI for a Limited period of time because of a Project	Employees with NO ACCESS to PHI (All PHI must be de-identified first)
<ul style="list-style-type: none"> <li>Director of Human Resources</li> <li>Assistant Director of Human Resources</li> <li>Deputy Director of Human Resources (aka Privacy Officer)</li> <li>Supervising Human Resources Analyst-Benefits</li> <li>Human Resources Analyst-Benefits</li> <li>Human Resources Technician – Benefits</li> </ul>	<ul style="list-style-type: none"> <li>Budget Analyst assigned to Human Resources</li> <li>Budget and Accountant assigned to Human Resources</li> <li>Payroll (coordinating paycheck contributions after plan enrollment)</li> <li>Mailroom staff</li> <li>Procurement Department staff during RFP for health benefits, have access to certain census and other group health plan data for underwriting purposes</li> <li>All other Human Resource staff not mentioned in this chart.</li> </ul>	<ul style="list-style-type: none"> <li>Assigned Audit staff</li> <li>All Information Technology Department staff</li> <li>Information Technology Officer (HIPAA Security Officer)</li> <li>Scanning staff</li> <li>City attorneys</li> <li>Temporary staff assigned to Human Resources</li> <li>Independent contractors</li> </ul>	<ul style="list-style-type: none"> <li>Housekeeping</li> <li>Building Maintenance</li> <li>All temporary staff</li> <li>All visitors</li> <li>All employees not listed as having some degree of access according to this chart.</li> </ul>

**NOTE: All the people in the columns shaded gray above deal with PHI and should be well versed (trained) in HIPAA privacy and security rules along with what is and is not permitted by the rules, since these people have been given permission to have PHI as a function of their work duties.**

4. Occasionally the Plan retains **temporary workers** to assist in group health plan administration. Such temporary workers will be informed of the Plan’s privacy policies and required to sign a confidentiality agreement before starting their work duties. Temporary worker access to PHI will be monitored and controlled.
5. The following chart outlines the **routine use and disclosure of PHI between this Plan and its Business Associates**. As long as these policies and procedures exist, the Plan does not need to make individual assessments of each routine use or disclosure. The Privacy Officer has determined that for routine disclosures related to payment or health care operations, the minimum necessary information may require more information than is provided in a limited data set.

See also the separate Business Associate vendor chart located in the pocket of the 3-ring binder for this Privacy Manual.

Business Associate (BA)	Eligibility, Enrollment & disenrollment information including SSN	Monthly, quarterly, annual Summary Reports on utilization, financial status, effectiveness of services rendered	Claim Appeals	Large Claim Report/ Stop Loss Reports	Case Management Reports	Other
Claims Administrators for the self-funded medical, dental, vision, Health FSA and COBRA benefits	X	X	X	X	X	

Business Associate (BA)	Eligibility, Enrollment & disenrollment information including SSN	Monthly, quarterly, annual Summary Reports on utilization, financial status, effectiveness of services rendered	Claim Appeals	Large Claim Report/ Stop Loss Reports	Case Management Reports	Other
PPO Network for the self-funded medical, dental and vision plans	X	X	X	X		
Utilization Management (UM) Company and Disease Management Company	X	X	X	X	X	
Prescription Benefit Management company (PBM)	X	X	X			
Independent Review Organization (IRO) for External Reviews			X			External Reviews
Employee Benefits Consulting firm	X	X	X	X	X	
Health Reimbursement Account Administrator	X	X	X			Health claims to determine reimbursement
Companies for maintaining and repairing computer systems for the group health plan						X
Companies for servicing and repairing photocopier and scanner used by the group health plan						X
Companies for shredding, recycling and destroying group health plan files						X
Companies for Electronic Data and Paper Data Storage						X

6. The Plan has identified the conditions appropriate for access to PHI, as follows:
- Plan staff must be trained in the Plan’s privacy policies and procedures before they may access PHI.
  - Plan staff must sign a confidentiality agreement before they may access PHI and renew every five years.
7. **Routine Disclosure of PHI:** The following are considered routine disclosures of PHI from the Group Health Plan and such disclosure may occur when the minimum necessary standard is applied:
- a. When information is disclosed to the Plan Sponsor (City Council/City Manager), the Plan will make reasonable efforts to de-identify the information or limit PHI to the minimum necessary to accomplish the intended purpose.
  - b. When receiving a request for PHI from one of the following categories of individuals, the Plan may rely on the judgment of the requestor as to the minimum amount of information that is necessary:
    - A public official or agency for a disclosure to them that is permitted under HIPAA. See also the Policy/Procedure on Disclosure of PHI for Public Health, Law Enforcement or Legal Process.
    - A health plan, health care clearinghouse, or health care provider that is covered by the HIPAA rules.

- A business associate (*see the Business Associate chart above*). NOTE: Business associate agreements should require a business associate to request from the Plan only the minimum information necessary to perform their functions on behalf of the Plan.
8. If staff is asked to disclose information that seems vague or is too broad, staff should seek clarification from the Privacy Officer before responding.
  9. Courier firms that transport packages/parcels with sealed PHI, such as the US Postal Service, UPS, FedEx, DHS and the like, are not considered to have routine access to PHI and are not considered to be Business Associates of the Plan.
  10. **Non-Routine Disclosure of PHI:**
    - a. A non-routine disclosure is a disclosure of PHI that is not addressed by the Routine Disclosure section noted above.
    - b. Each non-routine disclosure (that is not on a HIPAA-compliant authorization form or is more than the information in a limited data set) must be reviewed on an individual basis by the Privacy Officer. The criteria for reviewing a non-routine disclosure are as follows:
      - The non-routine disclosure must not be prohibited by the HIPAA privacy rules;
      - The non-routine disclosure must be necessary to allow the Plan to carry out its obligations under its governing plan documents;
      - The non-routine disclosure must be limited to the information minimally necessary to accomplish the purpose of the disclosure; and
      - The non-routine disclosure must be otherwise consistent with the Plan's privacy policies.
    - c. A request for a non-routine disclosure that is accompanied by an individual's written HIPAA-compliant authorization form will be honored in a manner consistent with the Plan's privacy policies. The information described in the authorization will be disclosed, even if that information is more than the limited data set information or is additional information that is reasonably necessary to accomplish the purpose of the disclosure.
  11. When requesting PHI from another health plan, health care provider or clearinghouse the Plan will make reasonable efforts to limit PHI to a limited data set (as defined in the policy section of this policy/procedures) and to information that is the minimum necessary to accomplish the intended purpose.
  12. When requesting medical records from a health care provider, the Plan will request only that portion of the medical records that is necessary to accomplish the intended purpose (e.g. just the emergency room record, not the entire hospital record). The Plan will use a HIPAA-compliant authorization form signed by the individual when requesting medical records from health care providers.
  13. The Plan will not request psychotherapy notes without written authorization from the individual. Psychotherapy notes are notes recorded in any medium by a health care provider who is a mental health professional documenting of analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes are only those notes that are kept separate from the rest of the medical record. Summary medical information regarding psychotherapy may be used without written authorization if for treatment, payment or health care operations purposes.
  14. In accordance with the HIPAA privacy rules, minimum necessary principles **do not** apply to the following uses, disclosures and requests for PHI:
    - a. Disclosures or requests to a health care provider for treatment purposes. The Plan does not generally engage in treatment. The Plan's services are limited to health care operations and payment. The treatment exception would generally only apply when information is requested by a health care provider for treatment purposes;
    - b. Disclosures to the individual who is the subject of the PHI. Identity of the individual must be verified (see the Verification Policy/Procedure);
    - c. Disclosures based on a HIPAA compliant authorization;
    - d. Disclosures to the Secretary of the Department of Health and Human Services (HHS) for compliance and enforcement purposes related to HIPAA's enforcement;
    - e. Uses or disclosures required by other laws; and
    - f. Uses or disclosures required for compliance with HIPAA's electronic data interchange (EDI) transaction standards. Any required or situational-required EDI elements do not have to meet the minimum necessary test. However, the minimum necessary standard does apply to optional data elements. Therefore, before including optional data elements in a HIPAA standard transaction the Plan may send or receive, the Plan must have a protocol for that use or disclosure.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.502.
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR VERIFICATION OF IDENTITY

---

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.514 (h) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

#### **General Policy:**

The Plan **must verify the identity of an individual or entity requesting Protected Health Information (PHI)**, and verify the authority of such individual to have access to PHI, before the PHI is disclosed to the individual, **if** the identity or any such authority of the individual is not known to the Plan.

The Plan will obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement or representation is a condition of disclosure of PHI under HIPAA. The Plan may rely, on their face, if such reliance is reasonable under the circumstances, on documentation, statements or representations that meet HIPAA's requirements.

#### **Identity of Public Officials:**

The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

If the request is in writing, the request is on the appropriate government letterhead; or

If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or
- If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

The verification requirements of this paragraph are met if the Plan relies on the exercise of professional judgment in making a use or disclosure.

#### **Emergency Situation: Imminent Serious Threat to Health and Safety:**

A disclosure to an individual or entity in accordance with section 164.512(j)(1)(i) (other than to a public official) to avert an imminent threat to health or safety is allowed without further verification if the Plan has a good faith belief that the disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, and the disclosure is to a person reasonably able to prevent or lessen the threat.

- If these conditions are met no further verification is needed.
- In such emergencies the Plan is not required to demand written proof that the person requesting the PHI is legally authorized.
- The Plan can reasonably rely on verbal representations.
- The Plan will document such disclosure.

**Where Verification is Not Required:**

This policy does not apply and verification is not required for disclosures made under section 164.510(a) regarding disclosures for facility directories, and 164.510(b) disclosures for involvement in an individual’s care and for notification purposes.

**KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

**PROCEDURES**

**1. When Required:**

Subject to any exceptions noted in this verification policy, unless an individual or entity is requesting PHI in person and the identity and authority of the individual or entity is personally known to Plan office representatives, the Plan must verify the identity and authority of the individual. Individuals are considered to have the authority to obtain their own PHI, [and (as included in this Plan’s HIPAA Privacy Notice), the PHI of their spouse and unemancipated minor children] unless otherwise indicated or such authority has been revoked in writing.

**2. Manner of Verifying Identity:**

- **Request in Person for Individual’s Own PHI:** If an individual makes a request for their own PHI in person, they must present the Plan with at least one piece of **acceptable identification** such as the employee’s ID number, driver’s license, employer issued picture ID card, school ID card, marriage certificate or divorce decree document, military ID card, adoption record, life insurance policy, passport or union card.

- **Request by Telephone or Electronically for Individual’s Own PHI:**

If an individual makes a request for his or her own PHI over the telephone or electronically, the individual must be able to verify their identity in accordance with the chart below, before the Plan will disclose PHI.

**Always verify the identity of an individual or entity requesting PHI before disclosing PHI. Whenever releasing someone else’s PHI to an inquirer, always limit the disclosure to the minimum necessary PHI.**

Who Claims to be Calling the Plan?	Data that is Available in the City of Stockton Human Resources Department to Verify Identity	Procedure to Verify Identity
<b>Employee</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Date of birth</li> <li>• Worksite department</li> <li>• Employee ID number</li> <li>• SSN</li> <li>• Hire date</li> </ul>	<p>Voice on the phone <b>must accurately verify</b> name, address, date of birth and worksite <u>plus</u> either employee ID number, SSN or hire date in order for City’s Human Resources staff to discuss the employee’s PHI with the caller. If verification not met, tell caller to come into the City’s Human Resources Department and bring photo ID.</p> <p>If employee is asking about PHI of a minor child or spouse, see the other rows of this chart.</p> <p>If employee is asking about PHI of a child age 18 years or older, instruct employee that the City’s Human Resources Department needs a Personal Representative designation form or Authorization form on file before being permitted to share such PHI. Tell employee where forms are located.</p>
<b>Retiree</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Date of birth</li> <li>• Former Worksite department</li> <li>• SSN</li> <li>• Termination/Retirement Date</li> </ul>	<p>Voice on the phone <b>must accurately verify</b> name, address, date of birth and former worksite <u>plus</u> SSN or termination date in order for City’s Human Resources staff to discuss the retiree’s PHI with the caller. If verification not met, tell caller to come into the City’s Human Resources Department and bring photo ID.</p> <p>If retiree is asking about PHI of a child or spouse, see the other rows of this chart.</p>

Who Claims to be Calling the Plan?	Data that is Available in the City of Stockton Human Resources Department to Verify Identity	Procedure to Verify Identity
<b>Spouse</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Date of birth</li> <li>• SSN</li> <li>• Date of Marriage</li> </ul>	<p>Voice on the phone must <b>accurately verify name</b>, address, date of birth, SSN and date of marriage in order for City’s Human Resources staff to discuss the spouse’s PHI with the caller. If verification not met, tell caller to come into the City’s Human Resources Department and bring photo ID.</p> <p>If spouse is calling about the PHI of the employee or child age 18 yrs or older, the City’s Human Resources Department needs to assure that the Plan’s HIPAA Notice has a section explaining how the Plan automatically honors a spouse as an employee’s personal representative and vice versa unless this automatic permission has been revoked in writing where the plan has received a Revoke A Personal Rep form before being permitted to share such PHI.</p>
<b>Child Under 18 Years of Age</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• SSN</li> <li>• Date of birth</li> </ul>	<p>If child can verify their own identity, we can release the child’s PHI to the child.</p> <p>Parents can have access to PHI on their children who are minors. (under age 18). Verify parent’s identity as per the row above on Employee, Retiree or Spouse.</p> <p><b>If Child is under age 18 years (including an emancipated child):</b> Normally okay to give PHI to the parent, <b>BUT</b>, if parent asking about any of these conditions where a <b>child is permitted to receive health care without parental consent</b>, the child may be entitled to his or her own PHI. Refer to the Privacy Officer for issues regarding: sexual/reproductive health care including contraceptives, sexually transmitted disease (STD), HIV, pregnancy, prenatal care, adoption, rape/sexual assault, abortion, or mental health and substance abuse (alcohol/drugs). Reference state minor consent laws.</p>
<b>Child Age 18 years or Older</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• SSN</li> <li>• Date of birth</li> </ul>	<p>Voice on the phone must accurately verify name, address, date of birth and SSN in order for City’s Human Resources staff to discuss the child’s PHI with the caller. If verification not met, tell caller to come into the City’s Human Resources Department and bring photo ID.</p> <p>If child is calling about the PHI of the employee, spouse or another covered child, the City’s Human Resources Department needs a Personal Representative designation form or Authorization form on file before being permitted to share such PHI. Tell caller where forms are located.</p>
<b>Ex-Spouse</b>	The City’s Human Resources Department may not have any data to verify identity.	Tell caller to come into the City’s Human Resources Department and bring photo ID. Do not release PHI about employee to the ex-spouse unless we have a signed Personal Representative or Authorization form.

Who Claims to be Calling the Plan?	Data that is Available in the City of Stockton Human Resources Department to Verify Identity	Procedure to Verify Identity
<b>Personal Representative (PR)</b>	Personal Representative form listing the name, address, phone number and password for the personal representative.	Locate the Personal Representative information in the City's Human Resources THE system and proceed to verify the caller's name, address, phone number and password before discussing PHI. If verification not met, tell caller to come into the City's Human Resources Department and bring photo ID.
<b>Business Associate (BA) (e.g., medical network, UM firm, consulting firm)</b>	Business Associate firm name and usual BA contact staff personnel and phone number or email address and signed BA agreement.	Can release/discuss the minimum necessary PHI with the Business Associate once verification of their identity is performed. If unable to verify identity, tell BA to email or write to the City's Human Resources department about their PHI needs/requests and the Privacy Officer will determine if such information can be released.  If PHI is not for treatment, payment or health care operations, or if no signed BA agreement exists, get an authorization form signed by the enrollee in order to release PHI to the BA.
<b>Health Care Provider</b>	The City's Human Resources Department may not have any data to verify identity.  Could search the health care provider's name, address and phone number to verify that what caller is saying is correct.	Caller wants PHI of their past, present or future patient, including information on Coordination of Benefits (COB): Once you have verified that the patient is in the City's Human Resources Department THE system, release the PHI needed to answer the specific question <u>only if</u> the question relates to Treatment, Payment or Health Care Operations. When in doubt, see the Privacy Officer.  Minimum Necessary standard does not apply to disclosures or requests by a provider for treatment.
<b>Manager/Supervisor</b>	Manager's name and department and office phone number	Caller wants PHI of an employee or a family member: Do not release PHI without a written authorization from the employee or the family member.
<b>Boyfriend or Girlfriend</b>	None	Caller wants PHI of an employee or employee's family member: Do not release PHI without a written authorization from the employee or the family member.
<b>Public Official or Law enforcement officer</b>	None  Ask for and copy badge information.	Request that they mail/fax or email the request for PHI to the Privacy Office and Privacy Officer will respond.  <i>Instructions to Privacy Officer:</i> Disclosure of PHI is subject to the policy and procedure on Disclosure of PHI for Public Health, Law Enforcement, or Legal Process. Retain the written proof of the request for PHI.

Who Claims to be Calling the Plan?	Data that is Available in the City of Stockton Human Resources Department to Verify Identity	Procedure to Verify Identity
<p><b>Employee’s family or close personal friend or other person involved in the care or payment for care of the individual.</b></p>	<p>First verify caller’s identity (name, relationship to patient).</p> <p>Second have caller identify patient by asking for:</p> <ul style="list-style-type: none"> <li>➤ Full name</li> <li>➤ Birth date</li> <li>➤ SSN</li> <li>➤ Address</li> <li>➤ Dates of service or location of patient</li> </ul>	<p>Caller is involved in the individual's care or payment for care: Refer to Privacy Officer.</p> <p><i>Instructions to Privacy Officer:</i> PHI can be disclosed to family member, relative, or close personal friend involved with the individual’s care or payment for care, provided the PHI is directly relevant to the person’s involvement with the individual’s health care or payment for health care. Generally, the individual must be given opportunity to agree or object to the disclosure.</p> <ul style="list-style-type: none"> <li>➤ Before releasing PHI contact the individual and ask whether or not they agree or object to release of PHI to the caller.</li> <li>➤ Ask individual about the person’s involvement in the individual’s care or payment for care.</li> <li>➤ If okay, release only info that is directly relevant to the person’s involvement in the care or payment for care. If caller is NOT involved in care or payment for care, then do not release PHI.</li> </ul> <p>Plan can release PHI to person who is not family member, relative, or close personal friend of the individual, if the Plan has reasonable assurance that the person has been identified by the individual as being involved in his or her care or treatment.</p>

- **Request by Mail or Fax for Individual’s Own PHI:** Any request for disclosure of PHI by mail or fax must be accompanied by a copy of at least one form of acceptable identification (as defined above) such that the Plan can determine if the address or fax number is the proper one for the individual requesting PHI disclosure. In addition, the Plan may choose to contact these individuals by telephone to confirm their identity.
- **Requests on Behalf of Another: PHI will not be disclosed to an individual (including another employee or supervisor)** requesting this information on behalf of another person, unless:
  - the individual is a personal representative of the individual (as set out in the Plan’s Personal Representative Policy) or
  - the Plan has a signed authorization form.

Plan staff will confirm the authority of a person to act on behalf of the individual by making sure that the personal representative procedure has been followed (i.e. a personal representative form has been completed indicating the authority of the individual to act on behalf of another). The individual acting on behalf of another must show their identity by providing an acceptable identification (as defined above).

Spouses and parents/guardians must also verify their relationship to the individual, in addition to verifying their identity, by providing a copy of a minor’s birth certificate, social security card, valid photo ID, etc.

For requests made over the telephone or electronically, the person acting on behalf of another must provide the information needed to verify identity to Plan staff.

- **Identifying Public Official:** The Plan will rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity of a public official or a person acting on behalf of a public official:
  - a. If the request is made in person, presentation of an agency identification badge, other official credential, or other proof of government status. Staff to record/document the identification that was presented.
  - b. If the request is in writing, the request is on appropriate letterhead (staff to make a copy); or

- c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official (staff to make a copy).
  - d. **Confirming Authority of Public Official:** The Plan will rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:
    - A written statement of the legal authority under which the PHI is requested, or if a written statement is impractical, an oral statement of such legal authority;
    - If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal, it is presumed to constitute legal authority.
  - **Requests by Other Parties:** When an entity (other than the individual themselves, a personal representative, or public official) requests disclosure of PHI that is otherwise allowed under HIPAA and the Plan's Policies and Procedures, the entity's identity and authority must also be confirmed.
    - An entity will be considered to have the authority to receive the PHI if a valid authorization is completed pursuant to the Plan's authorization policy.
    - To verify the identity of the entity, the Plan must receive a request for PHI and the authority by which the entity believes they are entitled to the PHI, in writing on the entity's letterhead (to assist the Plan in identifying that the entity is who they claim to be).
    - The Plan is not required to verify the identity and authority of an individual, business associate or other entity that is known to the Plan.
3. In the event staff are confronted with what they believe to be an **Emergency Situation** with Imminent Serious Threat to Health and Safety, staff will disclose PHI:
- to an individual or entity in accordance with section 164.512(j)(1)(i) (other than to a public official) to avert an imminent threat to health or safety is allowed without further verification if the Plan has a good faith belief that the disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, and
  - the disclosure is to a person reasonably able to prevent or lessen the threat.

If these conditions are met no further verification is needed.

In such emergencies the Plan is not required to demand written proof that the person requesting the PHI is legally authorized. The Plan can reasonably rely on verbal representations.

The Plan will document the disclosure of PHI, to whom with dates and times and what they believe constituted the Emergency Situation with Imminent Serious Threat to Health and Safety.

- 4. In the event staff are uncomfortable or uncertain that the presenting information is adequate verification according to this policy and procedure, staff will contact the Privacy Officer.
- 5. The Privacy Officer will retain documentation of verification records in accordance with the Plan's Record Retention policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.514(h).
- The Plan's Privacy Officer.
- Website referencing state laws on minor's right to consent:  
[https://www.gutmacher.org/statecenter/spibs/spib\\_OMCL.pdf](https://www.gutmacher.org/statecenter/spibs/spib_OMCL.pdf)

# HIPAA PRIVACY POLICY AND PROCEDURE FOR SAFEGUARDING PHYSICAL, ADMINISTRATIVE AND TECHNICAL PHI

---

---

## POLICY STATEMENT

This Policy and Procedure is adopted pursuant to section 164.530(c) of the Privacy Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

The Plan will establish appropriate procedures to safeguard PHI physically, administratively and technically. The Plan will take reasonable steps to limit incidental use or disclosure of PHI by anyone other than those individuals specifically authorized to work with PHI as part of Plan operations. Refer to the Plan's HIPAA Security Manual for more information on safeguarding of electronic PHI.

## KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

## PROCEDURES

The Plan will adhere to the following procedures for safeguarding PHI:

### 1. **E-mail Policy:**

The IT department has provided the Plan staff with a method to encrypt email using "Groupwise". The Privacy Officer may perform periodic audits of the e-mails of Plan staff to ensure that department e-mails are void of PHI or when PHI exists, the e-mails and attachments are properly encrypted.

2. **Security Protocols:** The Plan has designated the following security protocols for electronic or paper documents (including reporting a breach of confidentiality and disciplinary procedures for employees that breach confidentiality policies). The Plan's HIPAA Security Manual discusses security in more detail than this Privacy manual.

For documents stored on City network resources, access controls are based on IT requests from requestors that are authorized. There are shared areas where multiple people may have access. These resources should not contain documents with PHI in order to maintain HIPAA compliance.

Local electronic documents are maintain in accordance with HR policies.

- Plan computers are inventoried and serial numbers are recorded and maintained by the IT Department.
  - The City's Human Resources staff have locked file cabinets that are to be used to store all hard copy PHI.
  - No PHI is to be removed from the Plan City's Human Resources department, even on laptop, flash drive or other electronic means, except when appropriate for offsite storage.
  - The Privacy Officer will oversee the shipment of paper PHI from the Plan's City's Human Resources Department to the off-site storage to assure protection of PHI.
  - The Security Officer will oversee the shipment of electronic PHI from the Plan's City's Human Resources Department to the off-site storage to assure protection of PHI.
3. **Storage of PHI documents:** Paper documents containing PHI will be stored in the Plan's locked file cabinet(s) (meaning locked file cabinets in the Benefits section of the City's Human Resources Department) when not in immediate use. Plan file cabinets will not be used by departments **other than** group health plan staff. No document containing PHI will be left out on a desk overnight, unless the desk is in an office that can be and is also locked, in which case the documents with PHI will also not be left face up. No PHI documents are to be left on copier, fax and main workspace areas.
4. **Access to Plan Office:** Only Plan personnel will be given keys or key codes to enter the office. The Plan will monitor public access to the group health plan work areas. Visitors to the Plan's work area should be escorted and prevented from accessing PHI. The Plan is to make use of conference rooms, private offices and other secure areas in which to hold conversations involving PHI with non-Plan staff and visitors. Plan personnel who perform functions that requires access, use or disclosure of PHI work in physically segregated workspace. Other non-Plan personnel do not enter the segregated workspace unless accompanied by a Plan staff person.
5. **Computer Access:** The computer security controls of the Plan include a layered security approach to combine multiple mitigating security controls to protect Plan resources and data, including but not limited to firewalls, perimeter networking, intrusion detection systems, log review and consolidation, endpoint protections/anti-virus, anti-malware, application-level

security, backup, web browser security, zero day protection for software vulnerabilities and appropriate timely patches installed, encryption, etc.:

- A password is required to log onto a computer that allows access to group health plan benefit information.
- A user will be locked out after three invalid attempts to log into THE and Novell and six invalid attempts to log into GroupWise.
- Passwords must be at least seven (7) characters long with a combination of numbers, upper and lower case letters and special characters for GroupWise and Novell. For HTE, length requirement is 7-10 characters. Allowable characters are A-Z, 0-9, and characters \$, @, # and underscore. The password cannot begin with a number or special character. Passwords on the AS400 system are not case sensitive. Numbers cannot be next to each other. Characters cannot be repeated consecutively.
- Passwords must not be written down where others can find and use them and are not to be shared/provided to anyone else.
- Passwords must be changed every 90 days. New passwords cannot be the same as the past 12 prior passwords.
- Plan employees must not share their password information with anyone nor log onto the computer and then let others use that computer.
- City's Human Resources staff must lock their workstation when leaving the workstation.
- Computer workstations will automatically lock if activity does not occur for 15 or 30 minutes (as set by the user or set by IT at the system level) to prevent unauthorized access, and the password required to unlock.
- Manual workstation locking is accomplished by doing the following steps: Ctrl+Alt+Delete.
- Virus protection software on Plan computers is updated instantaneously and such software cannot be disabled by the user.
- Smart phones where plan staff can access email have remote wiping capability by IT personnel when lost/stolen.
- Regularly scheduled PC updates are installed.
- Emails are stored on a secure server with encryption.
- All PC's are locked down meaning that software cannot be installed without the approval and assistance of the IT personnel, minimizing transmission of a virus.
- Anti-virus software and security patches are installed and updated weekly to minimize possibility of malicious programs and spyware.
- Computer placement should prevent shoulder surfing. Privacy screens may be utilized.
- All computers in the City's Human Resources area are to be turned away from the doorway or walkway or staff will use a computer privacy screen filter cover to reduce the chance that a passerby might see PHI.
- Plan staff understand that password protecting Word and Excel files is not sufficient HIPAA protection, and only encryption is acceptable ePHI transmission security for our organization.
- Plan staff understand that efaxing, zipping and pdfing a document are not sufficient HIPAA protection and only encryption is acceptable ePHI transmission security for our organization.

6. **Fax:** Fax machines will be in secure locations and be monitored regularly (e.g. every 30 minutes) for incoming documents. To prevent receipt of incoming PHI to the dedicated fax machine when City's Human Resources staff are not available, fax machine(s) will be placed in a secure location where if PHI is sent after business hours, others cannot access such information.

All outgoing faxes must have a cover sheet with a confidentiality statement (see below for sample wording). Automatic pre-programmed fax dialing should be used on the fax machine (when possible) to help avoid incorrect dialing and sending of PHI to wrong locations.

*THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE. If the reader of this message is not the intended recipient or an employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the City of Stockton's Human Resources Department immediately by telephone at (209) 937-8233 and return the original message to us by mail. Thank you.*

7. **Discussion Areas for PHI:** Access to physical areas where Plan participants discuss PHI such as benefit issues/claim appeals/enrollment with Plan staff should be limited. Participants/Visitors will be directed to secure areas for conversations. Visitors are not to enter the Plan work area in order to minimize the chance of overhearing a PHI discussion or coming in contact with PHI of any form.

Plan staff are prohibited from discussing PHI in public areas such as the cafeteria, restroom, non-Human Resources Department locations, hallways, elevator, parking lot/garage, etc. A sign may be posted to alert visitors that the Plan will discuss PHI in private areas. The sign says:

**ATTENTION ALL EMPLOYEES AND VISITORS:**

*Our City's Human Resources Department is subject to Federal HIPAA privacy law. If you are here to discuss benefits information, have a personal health question, would like to discuss a health claim, claim appeal or other personal benefits business about yourself or your family, please allow us to first escort you to our confidential discussion room. We do not discuss personal health information in this public reception area. Thank you.*

8. **Computer Network:** Access controls (user-based, role-based and context based) are implemented and included in the administrative operations and system network controls. Firewalls are configured to provide the least privilege access. That is, to deny all and then allow minimal access to those people and systems that are authorized. Network traffic is directed to a specific system within the network.
9. **Workstation Inventory:** The Plan will maintain an inventory list/security log of the workstations that are considered Plan workstations, listing the date, type of workstation computer, model number, permitted user name(s) and server location(s). This will assist the Plan and Security Officer in tracking authorized users and assuring physical safeguards for these workstations.
10. **Termination of Employees:** Upon final departure of any terminated employees, the Plan will collect all keys and security cards and promptly change or disable the passwords of such terminated employees, including remote access.
11. **Electronic Transmission:** Because the City's Human Resources benefits administration staff do not have encryption of email, group health plan benefits administration staff understand that no emails can be responded to/replied to or created that contain any PHI and all emails must be de-identified in the email subject line, body of the email and in any attachments to any email within the Plan office, between staff working on PHI or through the internet.

The Plan understands that at this time, the HHS-specified technologies and methodologies to create **secure PHI** are:

- **Encryption for electronic PHI** "in motion," "at rest," and "in use." The Plan's encryption policies, if any, are described in its HIPAA Security Policies and Procedures.
  - **Destruction by shredding** for hardcopy PHI, whether documents, discs, tapes, flash drives or any other portable technology. Electronic PHI is destroyed in accordance with the applicable guidance issues by HHS. The Plan's Security Policies/procedures describe its procedures for the destruction of electronic PHI, if any.
12. **Disaster Recovery Program:** The Plan has a disaster recovery program for loss of data due to fire, vandalism, natural disaster, or other system failure. A backup tape will be created daily and stored in a secure temperature-controlled offsite location.
  13. **Business Continuity Plan:** is the Plan's roadmap for continuing operations under adverse conditions such as interruptions from natural disasters or man-made hazards like fire, vandalism, earthquake, flood, tornado, etc.
  14. **Shredding:** Documents containing PHI, which are not safely filed, will be shredded onsite before disposal using the cross-cut shredder or placing the documents in a locked shred bin. The privacy officer will assure that shred bins are locked and also that the shred bins are not filled so high as to permit removal of unshredded PHI documents. Files containing electronic PHI will be securely deleted according to IT Department standards. Hard drives are degaussed, erased and destroyed.

15. **Document Storage:** Documents containing PHI to be filed are to be sent to off-site storage in a sealed container. Storage boxes are labeled and inventoried. The Privacy Officer will assure that where PHI boxes are stored is not accessible by anyone other than Plan staff or a contracted business associate, such as an independent offsite storage firm. The boxes are picked up directly by the storage vendor who is a Business Associate to the plan.
16. **Hardware Disposal:** Prior to disposal of hardware that has been in the possession of/use by City's Human Resources staff the Information Technology Department staff will be notified so that hard drives of all computers and other electronic devices will be erased and destroyed so that no Plan PHI data remains and none can be recovered by any known recovery method. Disposal caution is taken for electronic devices including but not limited to desktops, laptops, notebooks, mobile devices, external hard drives, smart phones, flash drives, CDs/DVDs, hard drives inside of photocopiers/fax/similar devices used by Plan staff, scanning devices, etc.
17. **Internal Auditing:** The Plan reserves the right to internally audit the safeguard provisions in this policy/procedure, at a frequency determined by the Plan. The Privacy Officer will retain documentation of an internal audit finding for six years.
18. **Opening Mail:** Appropriate precautions will be taken when opening mail to assure that documents containing PHI are secure and viewed only by HIPAA trained Plan staff.
19. **Pictures Taken By Portable Devices:** There should be no reason that the Plan would take pictures or video recordings of an individual or any documents or computer screens with any portable device including but not limited to a camera or cell phone. If such a picture is needed in order to perform Plan business the Privacy Officer must be notified before taking a picture. At the direction of the Privacy Officer, the photo may need to be considered PHI.
20. **Remote and Mobile Access:** Plan employees have the option to remotely connect to the Plan network and access email and all software programs only through the Plan's secure virtual private network (VPN) or virtual desktop infrastructure (VDI) technology. Employees are to observe the same security precautions when working remotely as while working in the Plan office. Plan employees may also access emails via their company issued smartphone that contains encryption, PIN and password protection.

The following tips from the Federal government, on mobile device security, have been implemented by our Plan for Plan staff with certain mobile devices:

- a. For laptops, use a password or other user authentication.
- b. If email is linked, install and activate wiping and/or remote disabling to erase the data on the mobile device if it is lost or stolen.
- c. For laptops, install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks.
- d. For laptops, keep security software up to date.
- e. For laptops, maintain physical control of the mobile device. Know where it is at all times to limit the risk of unauthorized use.

The Plan's Privacy Officer will periodically review guidance issued by the government through this website for new information:

<http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security>.

21. **Shipping PHI:** The Plan understands that damaged shipping boxes and containers is a common way that PHI can be lost, damaged or compromised in transit. From time to time the Plan needs to ship PHI documents or electronic ePHI media, to an offsite storage location or to another Plan office or to a Business Associate. To help assure that the shipped PHI is safe, our Plan staff will take special care to pack the PHI by following these steps:
  - the inner box/bag will be enclosed in an outer box. Shipping boxes will not be loaded to weigh more than 25 pounds if possible to help reduce the chance the box is too heavy for transport vendors/USPS to lift and is dropped.
  - the outer box will be heavily taped.

Shipped PHI boxes/bags/containers will be insured for loss or damage up to the declared value of the contents, when possible.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions and Breach in this manual.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.530(c).
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR CERTIFICATION AND PLAN DOCUMENT AMENDMENT

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.504(f) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan Sponsor (who is named on the cover page of this manual) will provide written certification that the Plan Sponsor's Plan Documents have been amended to incorporate the requirements of the HIPAA Privacy regulation at section 164.504 (f) and that the Plan Sponsor agrees to comply with the Privacy Rules. This written certification will allow a health insurance issuer (hereafter called health insurance company), HMO, or the Group Health Plan (the Plan) to disclose individually identifiable health information to the Plan Sponsor for Plan Administration functions only.

The Plan can disclose PHI to the Plan Sponsor if the Plan Sponsor voluntarily agrees to use and disclose the information only as permitted or required by the regulation. PHI may be used only for plan administration functions (e.g. claim appeals) performed on behalf of the group health plan which are specified in plan documents.

**The Plan Sponsor's certification means** the Plan Sponsor agrees to:

1. Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
2. Ensure that any agents to whom the Plan Sponsor provides PHI received from the group health plan, agree to the same restrictions and conditions that apply to the Plan sponsor;
3. Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan sponsor;
4. Report to the group health plan any use or disclosure of PHI that is inconsistent with the plan documents or the HIPAA Privacy regulation;
5. Make the PHI accessible to individuals in accordance with 164.524 (Right of Access to PHI);
6. Allow individuals to amend their PHI in accordance with 164.526 (Right to Amend PHI);
7. Provide an accounting of PHI disclosures in accordance with 164.528 (Right to an Accounting of Disclosures);
8. Make the Plan's internal practices, books, and records relating to the use and disclosure of PHI received from the group health plan available to the Secretary of the Department of Health and Human Services (HHS) for determining compliance by the group health plan;
9. As feasible, return or destroy all PHI received from the group health plan when no longer needed; and
10. Ensure the establishment of adequate separation between the group health plan and the Plan Sponsor exists (e.g. firewalls) in accordance with 164.504(f)(2)(iii).

**Plan Documents will be amended** (in compliance with 164.504(f) requirements for group health plans) to:

- a. Establish permitted and required uses and disclosures of PHI by the Plan Sponsor;
- b. Provide that the Group Health Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification by the Plan Sponsor that the plan documents have been amended to incorporate the required elements.
- c. The required elements means that the text has been amended to address that the Plan Sponsor agrees to:
  - Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
  - Ensure that any agents to whom the Plan Sponsor provides PHI received from the group health plan, agree to the same restrictions and conditions that apply to the Plan sponsor;
  - Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan sponsor;
  - Report to the group health plan any use or disclosure of PHI that is inconsistent with the plan documents or the HIPAA Privacy regulation;

- Make the PHI accessible to individuals in accordance with 164.524 (Right of Access to PHI);
- Allow individuals to amend their PHI in accordance with 164.526) (Right to Amend PHI);
- Provide an accounting of PHI disclosures in accordance with 164.528); (Right to an Accounting of Disclosures);
- Make the Plan’s internal practices, books, and records relating to the use and disclosure of PHI received from the group health plan available to the Secretary of the Department of Health and Human Services (HHS) for determining compliance by the group health plan;
- As feasible, return or destroy all PHI received from the group health plan when no longer needed; and
- Ensure the establishment of adequate separation between the group health plan and the Plan Sponsor exists (e.g. firewalls) in accordance with 164.504(f)(2)(iii).
- Describe those employees or classes of employees or other persons under the control of the Plan Sponsor to be given access to PHI to be disclosed;
- Restrict the access to and use by the Plan Sponsor to plan administrative functions;
- Provide an effective mechanism for resolving any issues of noncompliance by employees or classes of employees or other persons under the control of the Plan Sponsor who have been given access to PHI.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Health Insurance Issuer** means (per Section 2791(b)(2) of the Public Health Service Act) an insurance company, insurance service, or insurance organization (including an HMO) which is licensed to engage in the business of insurance in a State and which is subject to State law which regulates insurance (within the meaning of section 514(b)(2) of ERISA. Such term does not include a group health plan.
- **Plan Sponsor** means the City of Stockton City Council/City Manager.
- **Plan administration functions** means administration functions (such as claim appeals) performed by the Plan Sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor. It does not include any employment-related functions or functions in connection with any other benefits or benefit plans not regulated by HIPAA Privacy.

## PROCEDURES

1. The Privacy Officer will assure that the Plan amends the applicable Plan Document(s) to be consistent with the use and disclosure of PHI permitted in the regulations.
2. The Privacy Officer will prepare a Certification Statement for the Plan Sponsor.
3. The Plan Sponsor will sign a written Certification Statement.
4. The original signed Certification Statement will be retained by the Privacy Officer.
5. Copies of the original certification statement may be provided by the Privacy Officer to interested parties as needed to prove that the Plan Sponsor voluntarily agrees to use and disclose the PHI only as permitted or required by the regulation.

## POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

## ADDITIONAL RESOURCES

- 45 CFR, Section 164.504 (f).
- The Plan’s Privacy Officer.

**City of Stockton  
Stockton, California**

**Certification to the Group Health Plan**

---

---

**This Certification is intended to comply with the HIPAA Privacy Rules, 45 C.F.R. §164.504(f) and 65 Fed. Reg. 82508 (December 28, 2000). This certification allows the City of Stockton’s City Council/City Manager (“Plan Sponsor”) and the City of Stockton’s Group Health Plan (“Health Plan”) to exchange protected health information (PHI) for plan administration functions without obtaining an individual’s authorization or consent.**

WHEREAS the City of Stockton City Council/City Manager is the sponsor of a group health plan for its employees and their dependents; and

WHEREAS Plan Sponsor’s group health plan is a “health plan” within the meaning of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH); and

WHEREAS the City of Stockton’s Group Health Plan (“Health Plan”) provides health insurance coverage to the participants and beneficiaries in the Plan Sponsor’s group health plan; and

WHEREAS Health Plan and Plan Sponsor desire to exchange health information protected under HIPAA (“protected health information” or “PHI”) for purposes related to administration of the group health plan;

THEREFORE BE IT RESOLVED, that Plan Sponsor hereby certifies to Health Plan the following, as required by 45 C.F.R. §164.504(f) of HIPAA:

The plan documents that govern the Plan Sponsor’s group health plan have been amended to incorporate the following provisions and Plan Sponsor agrees to:

- Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
- Ensure that any agents to whom it provides PHI received from Health Plan agree to the same restrictions and conditions that apply to Plan Sponsor with respect to such information;
- Not use or disclose PHI for employment-related actions and decisions;
- Not use or disclose PHI in connection with any other benefit or employee benefit plan of Plan Sponsor;
- Report to the Health Plan’s designee any PHI use or disclosure that it becomes aware of which is inconsistent with the uses or disclosures provided for;
- Make PHI available to an individual based on HIPAA’s access requirements;
- Make PHI available for amendment and incorporate any PHI amendments based on HIPAA’s amendment requirements;
- Make available the information required to provide an accounting of disclosures;

- Make its internal practices, books and records relating to the use and disclosure of PHI received from the Health Plan available to the Secretary of the U.S. Department of Health and Human Services to determine the Health Plan’s compliance with HIPAA;
- Ensure that adequate separation between the group health plan and the Plan Sponsor is established as required by HIPAA (45 CFR 164.504(f)(2)(iii)); and
- If feasible, return or destroy all PHI received from the Health Plan that the Plan Sponsor still maintains in any form, and retain no copies of such PHI when no longer needed for the specified disclosure purpose. If return or destruction is not feasible, the Plan Sponsor will limit further uses and disclosures to those purposes that make the return or destruction infeasible.
- Notify an individual if a breach of their unsecured protected health information (PHI) occurs.

---

This Certification signed at the City of Stockton, California this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_\_.

\_\_\_\_\_  
**City Manager for the Plan Sponsor**

\_\_\_\_\_  
**Privacy Officer for the City’s Group Health Plan**

## **PLAN DOCUMENT AMENDMENT**

### **Section 9.04 Health Insurance Portability and Accountability Act (HIPAA)**

#### **A. Introduction**

The City of Stockton (the Plan Sponsor) sponsors the following health plans:

1. The City of Stockton Medical Plans
2. The Employee Assistance Program (EAP)

In certain circumstances as described below, the Plan shall disclose to the Plan Sponsor Protected Health Information of Plan participants and other persons covered by the Plan (the Covered Individual).

The HIPAA of 1996, and the privacy regulations hereunder found at 45 C.F.R. Parts 160 and 164, as amended from time to time require the Plan to restrict the Plan Sponsor's ability to Use and Disclose Protected Health Information that is received from the Plan. One of the requirements is that the Plan Sponsor shall amend the Plan as set forth in 45 C.F.R. § 164.504(f)(2). In accordance with such requirements, the Plan was amended effective as of April 14, 2003. This Section contains that amendment. The Plan will not Use or Disclose Protected Health Information (PHI) to the Plan Sponsor in circumstances in which the HIPAA Privacy Rule would prohibit such Uses and Disclosures.

#### **B. Definitions**

1. The term "Business Associate" has the meaning set forth in 45 C.F.R. § 160.103.
2. The term "Disclose" or "Disclosure" means the release or transfer of, provision of access to, or divulging in any other manner individually identifiable health information to persons outside the Plan Sponsor.
3. The term "HIPAA Privacy Rule" means the applicable requirements of the privacy rules of Health Insurance Portability and Accountability Act of 1996 and related regulations, Title 45 Parts 160 and 164 of the Code of Federal Regulations, as amended from time to time.
4. The term "Plan Administration Functions" means administrative functions performed by the Plan Sponsor on behalf of the Plan and excludes functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor.
5. The term "Privacy Official" means the person who is responsible for the development and implementation of the HIPAA Privacy Rule policies and procedures of the Plan.
6. The term "Privacy Official" means the person who is responsible for the development and implementation of the HIPAA Privacy Rules policies and procedures of the Plan.
7. The term "Protected Health Information" (PHI) will have the meaning set forth in 45 C.F.R. § 164.501.
8. The term "Use" means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by the Plan Sponsor or any Business Associate of the Plan.

#### **C. Permitted Uses and Disclosures of Protected Health Information (PHI) by the Plan Sponsor**

##### **1. General**

The Plan will Disclose PHI to the Plan Sponsor only to enable the Plan Sponsor to carry out Plan Administration functions described in Section C.2 below, and such Disclosures shall be consistent with the requirement of the HIPAA Privacy Rule. The Plan will not Disclose PHI to the Plan Sponsor unless the Disclosures are explained in a Notice of Privacy Practices that is distributed to covered individuals.

##### **2. Description of Uses of Protected Health Information (PHI) by the Plan Sponsor**

The Plan may disclose PHI to employees of the Plan Sponsor solely for purposes of performing Plan Administration functions, and only to the extent necessary for such purposes. Such Plan Administration functions may include, but are not limited to, the design, administration, financial operations, or legal defense of the Plan. For example, PHI may be disclosed to the employees of the Human Resources Department to determine eligibility for Plan benefits and to facilitate the payment of benefits claims. PHI may also be disclosed to Appeals Hearing Committee Members, the City Manager, the City Attorney and their respective staff members in connection with a claim denial or an appeal and the Benefit Section Analyst in connection with a Use or Disclosure of PHI permitted or required by the HIPAA privacy rule. PHI may also be disclosed to the City Auditor, the Administrative Services Officer and their respective staff members for financial purposes such as reconciling bank accounts,

performing financial audits, and processing COBRA premium payments. The Plan Sponsor will not use or further disclose the PHI other than as permitted or required in accordance with this stated purpose or as required by applicable law.

#### D. Agents

The Plan Sponsor will ensure that any agents (including any subcontractors) to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to the PHI.

#### E. Employment Actions

The Plan Sponsor will not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan that is sponsored by the Plan Sponsor, except to the extent that such employee benefit plan is part of an organized health care arrangement (as defined in 45 C.F.R. § 164.501). The Plan and the EAP are part of an organized health care arrangement.

#### F. Reporting

The Plan Sponsor shall report to the Privacy Official any use or disclosure of information that is inconsistent with the purposes set forth in Section C above.

#### G. Access to the Information

The Plan Sponsor shall make PHI available to covered individuals for inspection and copying in accordance with 45 C.F.R. 164.524.

#### H. Amendment of PHI

The Plan Sponsor shall make PHI available to covered individuals for amendment and incorporate any amendment to PHI in accordance with 45 C.F.R. § 164.526.

#### I. Accounting of Disclosures of PHI

The Plan Sponsor shall make available the PHI required for the Plan to provide an accounting of disclosure of covered individuals in accordance with 45 C.F.R. § 164.528.

#### J. Information Available to the Secretary of Health and Human Services

The Plan Sponsor shall make its internal practices, books, and records relating to the Use and Discloser of PHI received from the Plan available to the Secretary of Health and Human Services for purposes of determining the Plan's compliance with the HIPAA Privacy Rule.

#### K. Return or Destroy PHI

If feasible, the Plan Sponsor will return or destroy all PHI received from the Plan that it maintains in any form and retain no copies of such information when no longer needed for the purpose for which the disclosure was made, except that, if such return or destruction is not feasible, the Plan Sponsor shall limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

#### L. Adequate Separation

1. The Plan Sponsor shall ensure that there is adequate separation between the Plan and the Plan Sponsor as required by the HIPAA Privacy Rule.
2. The following is a description of the employees or classes of employees or other persons under the control of the Plan Sponsor that shall be given access to PHI:
  - a. Human Resources Department: Director of Human Resources, Assistant Director of Human Resources, Deputy Director of Human Resources and their support staff.
  - b. Human Resources Department–Benefits Section: Analysts, Technicians, Specialists
  - c. Administrative Services Department: Administrative Services Officer, Supervising Accountant, Accountant and Administrative Analyst
  - d. City Manager, Deputy City Manager, and Executive Assistant
  - e. City Auditor, Senior Internal Auditor, Auditor I and II and Audit Assistant
  - f. City Attorney, Assistant City Attorney, Deputy City Attorney, and Secretary
  - g. Members of the Appeals Hearing Committee

3. The access to the use by the persons described in Section L.2 above shall be restricted to the Plan Administration functions that the Plan Sponsor performs for the Plan.
4. In the event there are any issues of noncompliance by the persons described in Section L.2, the Plan Sponsor shall take all necessary and appropriate action that is consistent with its disciplinary policy.

#### M. Certification by the Plan Sponsor

The Plan shall not disclose PHI to the Plan Sponsor unless the Plan Sponsor certifies that the Plan has been amended as required by the HIPAA Privacy Rule.

#### N. Miscellaneous

##### 1. Rights

This Section 9.04 shall not be construed to establish requirements or obligations beyond those required by the HIPAA Privacy Rule. Any portion of this Amendment that appears to grant any additional rights not required by the HIPAA Privacy Rule shall not be binding upon the Plan Sponsor.

##### 2. Amendment

The Plan Sponsor reserves the right to amend or terminate any and all provisions set forth in this Amendment at any time to the extent permitted under the HIPAA Privacy Rule.

##### 3. Delegation

The Plan Sponsor may delegate or allocate any authority or responsibility with respect to this amendment. The Plan Sponsor (or its delegate) has the discretion to construe and interpret the terms, provisions, and requirements of this amendment. All decisions of the Plan Sponsor (or its delegate) with respect to this amendment shall be given the maximum deference permitted by law.

##### 4. Document Retention

If a communication under this amendment is required by the HIPAA Privacy Rule to be in writing, the Plan Sponsor shall maintain such writing, or electronic copy, as documentation.

If an action, activity, or designation is required by the HIPAA Privacy Rule to be documented, the Plan Sponsor shall maintain a written or electronic record of such action, activity or designation. The Plan Sponsor shall retain the required documentation for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

##### 5. Construction

The terms of this amendment shall be construed in accordance with the requirements of the HIPAA Privacy Rule and in accordance with any applicable guidance on the HIPAA Privacy Rule issued by the Department of Health and Human Resources.

#### O. In compliance with HIPAA Security regulations, the Plan Sponsor will:

1. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of the group health plan,
2. Ensure that the adequate separation discussed in L above, specific to electronic PHI, is supported by reasonable and appropriate security measures,
3. Ensure that any agent, including a subcontractor, to whom it provides electronic PHI agrees to implement reasonable and appropriate security measures to protect the electronic PHI, and
4. Report to the Plan any security incident of which it becomes aware concerning electronic PHI.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR BUSINESS ASSOCIATES

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 160.103, 164.502(e), 164.504, and 164.532 of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

- A. The Plan will coordinate a business associate contract or other arrangement as required by the HIPAA Privacy regulations.
- B. The contract between the Plan and a business associate will:
  1. Establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate. The contract will not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the regulations, except that:
    - a. The contract may permit the business associate to use and disclose protected health information (PHI) for the proper management and administration of the business associate; and
    - b. The contract may permit the business associate to provide data aggregation services relating to the health care operations of the Plan.
  2. Provide that the business associate will:
    - a. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
    - b. Use appropriate safeguards to prevent use or disclosure of the information, including electronic protected health information, other than as provided for by its contract;
    - c. Report to the Plan any use or disclosure of the information not provided for by its contract of which it becomes aware including breaches of unsecured protected health information;
    - d. Ensure that any agents to whom it provides protected health information received from, or created or received by the business associate on behalf of, the Plan agree to the same restrictions and conditions that apply to the business associate with respect to such information;
    - e. Make available protected health information in accordance with § 164.524 (regarding access of individuals to PHI);
    - f. Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526 (regarding amendment of PHI);
    - g. Make available the information required to provide an accounting of disclosures in accordance with § 164.528 (regarding accounting of disclosure of PHI);
    - h. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the Plan available to the Secretary for purposes of determining the Plan's compliance with this subpart; and
    - i. At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the Plan that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
  3. **Violation of Privacy by Business Associate:** If the Plan knows of a pattern of activity or practice of a business associate or a subcontractor of the business associate that constitutes a material breach or violation of the business associate's or subcontractor's obligation under the contract or other arrangement, the Plan will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Plan reserves the right to terminate the contract or arrangement, or if termination is not feasible, report the problem to the Secretary for the Department of Health and Human Services.
  4. If a Plan and its business associate are both governmental entities, the Plan may comply with the business associate contract requirements by entering into a memorandum of understanding (MOU) with the business associate that contains terms that accomplish the objectives of paragraph 2 above.

5. The contract or other arrangement between the Plan and business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the Plan, if necessary for the proper management and administration of the business associate; or to carry out the legal responsibilities of the business associate.
6. The contract or other arrangement between the Plan and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for disclosures required by law; or:
  - a. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
  - b. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
  - c. The requirements of a business associate agreement apply to the contract or other arrangement between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.
7. The Plan will assure that a Business Associate contract is signed with each business associate of the Plan prior to April 14, 2003 unless the provisions below, apply.
8. If the Plan has entered into a Business Associate contract prior to January 25, 2013, the Plan will revise the Business Associate contract in accordance with HIPAA Omnibus regulations and will have until the earlier of (a) the date such contract is renewed or modified on or after September 23, 2013, or (b) until September 22, 2014.
9. The Plan will, in some instances, implement an extension of time for executing Business Associate contracts. Extensions must be approved by the Privacy Officer according to the following parameters:
  - a. If there is an existing, signed contract between the Plan and a Business Associate prior to October 15, 2002, a Business Associate contract is not necessary until April 14, 2004.
  - b. If there is any change in the signed contract between the Plan and a Business Associate, including a fee change, then a Business Associate contract will be executed at the same time the existing contract is modified.
  - c. Regardless of whether a Business Associate Agreement has been obtained, the Plan will comply with the individual rights provisions of HIPAA (as applicable) and will permit the Secretary of Health and Human Services to inspect records.
10. The Plan will assure that a Business Associate contract is obtained for all new Business Associate relationships acquired after April 14, 2003. The Plan will assure that Business Associate contracts are updated in compliance with step 8 above.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- A. **Business Associate (BA)** means, with respect to a covered entity (the Plan), a person who:
  - a. On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20 (*outlined under Patient Safety Activities below*), billing, benefit management, practice management, and repricing; or
  - b. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 *which is defined below*), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

**Patient safety activities** means the following activities carried out by or on behalf of a Patient Safety Organization (PSO) or a provider:

- (1) Efforts to improve patient safety and the quality of health care delivery;
- (2) The collection and analysis of patient safety work product;

- (3) The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;
- (4) The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;
- (5) The maintenance of procedures to preserve confidentiality with respect to patient safety work product;
- (6) The provision of appropriate security measures with respect to patient safety work product;
- (7) The utilization of qualified staff; and
- (8) Activities related to the operation of a patient safety evaluation system (the collection, management, or analysis of information for reporting to or by a Patient Safety Organization) and to the provision of feedback to participants in a patient safety evaluation system.

**Data aggregation**, is where a business associate in its capacity as the business associate of one covered entity combines the protected health information of such covered entity with protected health information received by the business associate in its capacity as a business associate of another covered entity in order to permit the creation of data for analyses that relate to the health care operations of the respective covered entities.

**Disclosure** means the release, transfer provision of access to, or divulging in any manner of information outside the entity holding the information.

B. A covered entity may be a business associate of another covered entity.

C. **Business associate includes:**

- a. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
- b. A person that offers a personal health record to one or more individuals on behalf of a covered entity.
- c. A **subcontractor** that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

D. Business associate **does not** include:

- a. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
- b. A Plan Sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the Plan Sponsor, to the extent that the requirements of § 164.504(f) (*meaning the Business Associate contract provisions*) apply and are met.
- c. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
- d. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (A-a in this definition) for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (A-b in this definition) of this definition to or for such organized health care arrangement by virtue of such activities or services.

- **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.
- **Organized health care arrangement** means:
  1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
  2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint activities that include at least one of the following:
    - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    - Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plans each of which are maintained by the same Plan Sponsor;  
or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

## PROCEDURES

1. The Privacy Officer will identify and retain a list of Business Associates of the Plan.
2. Starting February 1, 2013 and prior to September 23, 2013, the Privacy Officer will investigate whether certain vendors used by the Plan have become Business Associates because of the HIPAA Omnibus regulations redefined definition of business associate, such as a personal health record vendor or a cloud storage vendor, and if so, the Plan will obtain a business associate contract with the vendor.
3. If the Plan has entered into a Business Associate contract prior to January 25, 2013, the Plan will revise the Business Associate contract in accordance with HIPAA Omnibus regulations and will have until the earlier of (a) the date such contract is renewed or modified on or after September 23, 2013, or (b) until September 22, 2014, as noted below:

Status of BA Agreement	Action Steps on Updating a BA Agreement to Comply with HIPAA Omnibus Regulations
HIPAA compliant BA agreement in effect before 1-25-13 and is renewed or modified on or after 1-25-13 and before 3-26-13.	If it's an evergreen or automatically renewed contract with no changes/modifications, update the BA agreement no later than 9-22-14. If it is unclear, best to update the BA agreement by 9-23-13.
HIPAA compliant BA agreement in effect before 1-25-13 and is renewed or modified during the period 3-26-13 and 9-23-13.	Update the BA agreement by 9-23-13.
HIPAA compliant BA agreement in effect before 1-25-13 and is NOT renewed or modified during the period 3-26-13 and 9-23-13.	Update the BA agreement on the earlier of the renewal/modification date or 9-22-14.
HIPAA compliant BA agreement in effect before 1-25-13 and is renewed or modified on or after 9-23-13.	Update the BA agreement on the earlier of the renewal/modification date or 9-22-14.
New BA agreement executed in 2013 but before 9-23-13.	Update the BA agreement by 9-23-13.
New BA agreement executed on or after 9-23-13.	Update the BA agreement by the effective date of the agreement.
No BA agreement in place with Business Associate on or before 1-25-13.	Update the BA agreement ASAP and definitely by 9-23-13.

4. In the absence of a Business Associate contract received from a Business Associate, the Privacy Officer will work with legal counsel to develop a Business Associate contract for the Plan's use that is in compliance with the HIPAA regulations at 164.504(e) and the 2013 HIPAA Omnibus regulations. The Plan will seek legal counsel support for business associate contract creation and contract revisions.
5. The Privacy Officer will manage the process of assuring that the Plan has a valid signed Business Associate contract with each existing and new Business Associate within the timeframes outlined in the policy above at steps 7 and 8.

When the Plan seeks a formal competitive bid process it will assure that the Request for Proposal stipulates the need for a Business Associate relationship and work with the Procurement Department on Business Associate contracts for newly hired vendors who will be Business Associates of the Plan.

6. The Privacy Officer will assure that follow-up calls are made to Business Associates on at least a monthly basis to review the status of any **unsigned** Business Associate contracts. The Plan understands that it cannot share PHI with a Business Associate unless and until a Business Associate contract is fully executed. Also, the Plan understands that it cannot share PHI with a subcontractor of a Business Associate unless and until a Business Associate contract is fully executed between the subcontractor and the Business Associate.

7. If Business Associates have questions regarding Business Associate contract language, the Business Associate will be referred to the Privacy Officer or the Plan's legal counsel.
8. When a Business Associate returns an executed copy of the Business Associate contract, the Privacy Officer will retain a copy and forward the original signed copy to the City Clerk.
9. Plan staff who identify a breach of contract by a Business Associate, such as an issue noted in B-2 of the policy section of this document, should address it with the Business Associate in writing and notify the Plan's Privacy Officer. The Privacy Officer will take steps to document contact with the Business Associate regarding the breach and seek assurance from the Business Associate that protocol is in place to prevent further breach. The Privacy Officer will consult with legal counsel as necessary.
10. The Privacy Officer will retain documentation of Business Associate contracts and discussion of any breach, as required by the Plan's Policy on Record Retention.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 160.103, 164.502(e), 164.504 and 164.532.
- The Plan's Privacy Officer.

## SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

### Health Insurance Portability and Accountability Act (HIPAA) Appendix to the Preamble

67 Fed. Reg. 53264-53266 (August 14, 2002)

*Note: This Sample Business Associate Agreement contains language published by the Department of Health and Human Services in the Federal Register on August 14, 2002. This model was used from April 2002 thru January 2013. For BA agreements used after January 2013, see the next attachment, which is the new model BA agreement incorporated as part of the 2013 HIPAA Omnibus regulations. Legal counsel should review all Business Associate Agreements.*

#### **Statement of Intent**

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate. These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement.

These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract. Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule.

For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

#### ***SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS***

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

#### **Definitions (Alternative Approaches)**<sup>1</sup>

##### Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

##### Examples of specific definitions:

- (a) Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].
- (b) Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
- (c) Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- (d) Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
- (e) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

---

<sup>1</sup> Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these model provisions and are not intended to be included in the contractual provisions.

- (f) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.
- (g) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

### ***Obligations and Activities of Business Associate***

- (a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- (c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
- (d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
- (e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]
- (g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]
- (h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- (i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- (j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

## ***Permitted Uses and Disclosures by Business Associate***

### **General Use and Disclosure Provisions (alternative approaches)**

**Specify purposes:** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: [List Purposes].

**Refer to underlying services agreement:** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

### **Specific Use and Disclosure Provisions: [only necessary if parties wish to allow Business Associate to engage in such activities]**

- (a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- (b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).
- (d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

### **Obligations of Covered Entity Provisions for Covered Entity To Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]**

- (a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

### **Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

### **Term and Termination**

- (a) **Term**. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]
- (b) **Termination for Cause**. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the \_\_\_ Agreement/ sections \_\_\_ of the \_\_\_ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; (2) Immediately terminate this Agreement [and the \_\_\_ Agreement/ sections \_\_\_ of the \_\_\_ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or (3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. [Bracketed language in this provision may be necessary if there is an underlying services Agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]
- (c) **Effect of Termination**.
  - (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
  - (2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

### **Miscellaneous**

- (a) **Regulatory References**. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- (b) **Amendment**. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- (c) **Survival**. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to ``Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
- (d) **Interpretation**. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

**SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS**  
(Published January 25, 2013)

**INTRODUCTION APPEARING ON THE HHS WEBSITE:**

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>

*A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information.*

*A “business associate” also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.*

*The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate.*

*A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law.*

*A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law.*

*A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.*

*A written contract between a covered entity and a business associate must:*

- (1) establish the permitted and required uses and disclosures of protected health information by the business associate;*
- (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law;*
- (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information;*
- (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;*
- (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity’s obligation with respect to individuals’ requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;*
- (6) to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;*
- (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity’s compliance with the HIPAA Privacy Rule;*
- (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity;*
- (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and*
- (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.*

*This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.*

***This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor.***

*In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement.*

*These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract.*

***Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.***

*See next page for the government-provided model BA agreement.*

***Legal counsel should review all Business Associate Agreements.***

## **Sample Business Associate Agreement Provisions**

*For use on or after January 25, 2013*

*Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.*

*Legal counsel should review all Business Associate Agreements.*

### **Definitions**

#### Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

#### Specific definitions:

- (a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].
- (b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].
- (c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

### **Obligations and Activities of Business Associate**

Business Associate agrees to:

- (a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
- (b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
- (c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

- (d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;
- (e) Make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

- (f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

- (g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

- (h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and
- (i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

#### **Permitted Uses and Disclosures by Business Associate**

- (a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

- (b) Business associate may use or disclose protected health information as required by law.
- (c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

- (d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]
- (e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.
- (f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

#### **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

- (a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.
- (b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.
- (c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

#### **Permissible Requests by Covered Entity**

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

#### **Term and Termination**

- (a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.
- (b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered

entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1.

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under “Permitted Uses and Disclosures By Business Associate”] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate’s obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

**Miscellaneous [Optional]**

- (a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- (b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.
- (c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR USE AND DISCLOSURE OF PHI AS REQUIRED BY LAW

- **FOR PUBLIC HEALTH ACTIVITY;**
- **FOR VICTIMS OF ABUSE, NEGLECT OR DOMESTIC VIOLENCE;**
- **FOR HEALTH OVERSIGHT ACTIVITIES;**
- **FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS (e.g. SUBPOENA);**
- **FOR LAW ENFORCEMENT PURPOSES (e.g. DECEASED, CORONER, FUNERAL DIRECTOR, ORGAN PROCUREMENT, ETC.);**
- **FOR RESEARCH;**
- **TO AVERT A THREAT TO HEALTH OR SAFETY; AND**
- **FOR SPECIALIZED GOVERNMENT FUNCTIONS (e.g. National Security).**

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.512 of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

**The Plan may use and disclose Protected Health Information (PHI)** as required by the law and for Public Health Activity, Victims of Abuse, Neglect or Domestic Violence, Health Oversight Activities, Judicial and Administrative Proceedings, Law Enforcement, Research, to Avert a Serious Threat to Health or Safety, or for Specialized Government Functions purposes **without the written authorization of the individual who is the subject of the information and the Plan is not required to give the individual the opportunity to agree or object to the use or disclosure.**

#### Uses And Disclosures Required By Law:

The Plan may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. The Plan must meet the requirements (described below) for:

- victims of abuse, neglect or domestic violence;
- judicial and administrative proceedings; and
- law enforcement purposes.

#### Disclosures For Public Health Activity:

The Plan may use or disclose PHI for the public health activities and purposes noted below:

- a. to a public health authority authorized by law to collect or receive PHI **for the purpose of preventing or controlling disease, injury or disability.** This includes but is not limited to the following:
  - Reporting disease or injury;
  - Reporting vital events such as birth or death;
  - Conducting public health surveillance, investigations or interventions; or
  - At the direction of a public health authority to an official of a foreign government agency that is acting in collaboration with a public health authority.
- b. to a public health authority or other appropriate government authority authorized by law to receive **reports of child abuse or neglect.**
- c. to a person subject to the **jurisdiction of the Food and Drug Administration (FDA)** with respect to an FDA-related product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:
  - To collect or report adverse events, product defects or problems or biological product deviations;
  - To track FDA-regulated products;

- To enable product recalls, repairs or replacement or look back (locating and notifying individuals who have received products that have been recalled, withdrawn or are the subject of the look back); or
  - To conduct post-marketing surveillance.
- d. to notify a **person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition** if the Plan or public health authority is authorized by law to notify such person as necessary to conduct a public health intervention or investigation.
- e. to an employer about an individual who is a member of the workforce of the employer if the covered entity is a covered health care provider who provides health care to the individual at the request of the employer to conduct an evaluation relating to **medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury**.
- The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance.
  - The employer needs such findings in order to comply with its obligations under 29 CFR 1904-1928 (Recording and reporting occupational injuries and illnesses), 30 CFR parts 50-90 (Mine safety and health) or state law.
  - The covered health care provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided or if the health care is provided on the worksite, by posting the notice in a prominent place at the location where the health care is provided.
- f. to a school about an individual who is a student or prospective student of the school if the protected health information this is disclosed is **limited to proof of immunization**, the school is required by State or other law to have such proof of immunization prior to admitting the individual and the covered entity obtains and documents the agreements to this disclosure from either a parent, guardian or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or the individual, if the individual is an adult or emancipated. *(HHS notes the important role schools play in preventing communicable diseases and that most states have laws that prohibit a student from attending school unless the school had received the student's immunization records. Accordingly, the Omnibus rule amended the section on public health activities to permit a covered entity, like the Plan, to disclose proof of immunization (without a written authorization) to a school where state or other law requires the school to have such information prior to admitting the student.)*

#### **Disclosures For Victims Of Abuse, Neglect Or Domestic Violence:**

Except for reports of child abuse or neglect (as discussed above under Public Health Activity, letter b), the Plan may disclose PHI about an individual whom the Plan reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence. Disclosure will be made only:

- a. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law;
- b. If the individual agrees to the disclosure; or
- c. To the extent the disclosure is expressly authorized by statute or regulation and the Plan, in the exercise of professional judgment, believes the disclosure is necessary to prevent further harm to the individual (victim) or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

**The Plan will promptly inform an individual of any disclosure** noted above unless the Plan believes that informing the individual would place the individual at risk of serious harm, or if the Plan would be informing a personal representative who the Plan believes is responsible for the abuse or injury and informing the representative would not be in the best interests of the individual.

### **Disclosures For Health Oversight Activities:**

The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative or criminal proceedings or actions or other activities necessary for appropriate oversight of:

- a. the health care system;
- b. government benefit programs for which health information is relevant to beneficiary eligibility;
- c. entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- d. entities subject to civil rights laws for which health information is necessary for determining compliance.

**Health oversight activity does not include** (and the Plan will not disclose PHI for) an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- receipt of health care;
- a claim for public benefits related to health; or
- qualification for or receipt of public benefits or services when a patient's health is integral to the claim for public benefits or services.

### **Disclosure For Judicial And Administrative Proceedings (e.g. subpoena):**

The Plan may disclose PHI in the course of any judicial or administrative proceeding as follows:

- a. in response to **an order of a court** or administrative tribunal (provided that the Plan discloses only the PHI expressly authorized by such order); or
- b. in response to a **subpoena**, discovery request or other lawful process that is **not** accompanied by an order of the court or administrative tribunal, if:
  - the Plan receives "satisfactory assurance" from the party seeking PHI that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request in accordance with the definition of satisfactory assurance in compliance with section 164.512 (e)(1) (iii) that:
    - the individual has been given notice of the request and the Plan receives from that party a written statement and accompanying documentation demonstrating that the party requesting the PHI has made a good faith attempt to provide written notice to the individual (or mail to the last known address); and
    - the Notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and the time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or all objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution; or
  - The Plan receives "satisfactory assurance" from the party seeking the PHI that reasonable efforts have been made by the party to secure a "qualified protective order" (as defined below), if:
    - the Plan receives from the party a written statement and accompanying documentation demonstrating that the parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
    - the party seeking the PHI has requested a "qualified protective order" from such court or administrative tribunal.

### **Disclosure For Law Enforcement Purposes:**

The Plan may disclose PHI for a law enforcement purpose to a law enforcement official if the following conditions are met:

- a. As required by law(s) that **require reporting of certain types of wounds or other physical injuries**;
- b. In compliance with and as limited by the requirements of:
  - a **court order or court-ordered warrant**;
  - a **subpoena or summons** issued by a judicial officer;
  - a **grand jury subpoena**; or
  - an **administrative request**, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process under law provided that the PHI sought is relevant to a legitimate law

enforcement inquiry, the request is specific and limited to the purpose for which the information is sought, and de-identified information could not be used.

- c. The Plan may disclose PHI about an individual 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, but the Plan may disclose only the following information:**
- Name and address;
  - Date and place of birth;
  - Social security number;
  - ABO blood type and Rh factor (if known);
  - Type of injury;
  - Date and time of treatment;
  - Date and time of death, if applicable; and
  - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- The Plan may not disclose for the purposes of identification or location, any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.
- d. The Plan may disclose PHI in response to a law enforcement official's request about an individual who is (or is suspected to be) **a victim of a crime** if:
- The individual agrees to such disclosure, or
  - The Plan is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
    - the law enforcement official represents that the PHI is needed to determine whether a violation of law by someone other than the victim has occurred, and that such information is not intended to be used against the victim, that immediate law enforcement activity which depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and
    - that the disclosure of PHI is in the best interest of the individual.
- e. The Plan may disclose **PHI about an individual who has died** to a law enforcement official if the Plan suspects the individual's death may have resulted from criminal conduct.
- f. 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 covered entity.
- g. The Plan may disclose PHI to **a coroner or medical examiner** for the purpose of identification of a deceased person, determining a cause of death, or other duties as authorized by law.
- h. The Plan may disclose PHI to **funeral directors** as necessary to carry out their duties with respect to a deceased individual or if necessary, PHI may be disclosed prior to and in anticipation of the individual's death.
- i. The Plan may disclose PHI to **organ procurement organizations** or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

#### **Disclosure For Research Purposes:**

The Plan may provide PHI for research (regardless of the source of funding for the research) if:

- The Plan obtains an alteration to or waiver of the authorization for use or disclosure of PHI that has been approved by an Institutional Review Board (IRB) or a privacy board (as defined in 164.512(I)(1)(B)).
- The Plan must also receive representation from the researcher(s) that use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or similar purpose, and that no PHI will be removed from the Plan by the researcher in the course of the review, and the PHI is necessary for research purposes.
- **Research on decedents:** The Plan must obtain from the researcher representation that the use and disclosure is solely for research on the PHI of decedents, documentation of the death of such individuals and representation that the PHI is necessary for research purposes.
- **Waiver of Authorization:** For use and disclosure of PHI to be permitted based on documentation or approval of an alteration or waiver of authorization, the documentation must include all the following:
  - A statement identifying the IRB or privacy board and the date the alteration or waiver was approved.
  - A statement that the IRB or privacy board has determined that the alteration or waiver of authorization satisfies the following criteria:

- a. use or disclosure of PHI involves no more than minimal risk to the privacy of individuals based on at least the presence of an adequate plan to protect the identifiers from improper use and disclosure;
  - b. an adequate plan to destroy the identifiers at the earliest opportunity; and
  - c. written assurance that the PHI will not be reused or disclosed except as required by law, for authorized oversight of the research study.
- The research could not practically be conducted without the waiver or alteration and could not be conducted without access to the PHI.
  - A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board.
  - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures in compliance with 164.512 (i) (2)(iv).
  - Documentation of the alteration or waiver of authorization must be signed by the chair or other member as designated by the chair of the IRB or privacy board.

**Disclosure To Avert A Serious Threat To Health Or Safety:**

The Plan may (consistent with applicable law and standards of ethical conduct) use and 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 or safety of a person or the public and is to a person(s) reasonably able to prevent or lessen the threat or
- Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

The Plan CANNOT disclose PHI relating to an individual’s therapy or request for therapy to treat a propensity to commit the criminal conduct that is the basis for the disclosure (164.512 (j)(2)).

When the Plan can disclose PHI, such information is to be limited (in accordance with 164.512 (f)(2)(i)) that indicates the Plan may only disclose the following:

- a. Name and address;
- b. Date and place of birth;
- c. Social security number;
- d. ABO blood type and Rh factor;
- e. Type of injury;
- f. Date and time of treatment;
- g. Date and time of death, if applicable; and
- h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

The Plan may not disclose for the purposes of identification or location any PHI related to the individual’s DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

**Disclosures For Specialized Government Functions (e.g. National Security):**

- a. The Plan may disclose PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the military authority has published in the *Federal Register* the appropriate military command authorities; and the purposes for which the PHI may be used or disclosed.
- b. The Plan may disclose PHI to authorized Federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333). The Plan may also disclose PHI to officials for the protection of the President or other persons or to foreign heads of state 164.512 (k)(3).
- c. The Plan may disclose PHI to Correctional Institutions and other law enforcement custodial situations having lawful custody of an inmate or other PHI of an inmate or individual if the correctional institution or law enforcement official represents that such PHI is necessary for:
  - The provision of health care to such individual;
  - The health and safety of such individual or other inmates;
  - The health and safety of the officers or employees of or others at the correctional institution or those persons responsible for the transporting of inmates or their transfer from one institution, facility or setting to another;
  - Law enforcement on the premises of the correctional institution; or

- The administration and maintenance of the safety, security and good order of the correctional institution.

An individual is no longer an inmate when released on parole, probation, supervised release or otherwise is no longer in lawful custody.

- d. A health plan that is a state or local government program providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies (or the maintenance of such information in a single or combined data system accessible to all such government agencies) is authorized by statute or regulation, is necessary to coordinate the covered functions of such programs, or is necessary to improve management of such programs.

### **Workers' Compensation 164.512 (l):**

The Plan may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

### **KEY DEFINITIONS**

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Satisfactory assurance means** (in compliance with 164.512 (e) (1) (iii)) that the Plan receives from the party a written statement and accompanying documentation that the party requesting such information has made a good faith attempt to provide written notice to the individual, the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and the time for the individual to raise an object has elapsed and no objections were filed or all objections filed have been resolved by the court or administrative tribunal and disclosures are consistent with such resolution.
- **Satisfactory assurance means** (in compliance with 164.512 (e) (1) (iv)) that the Plan receives from the party a written statement and accompanying documentation demonstrating that the parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
- **Qualified protective order means** (in compliance with 164.512 (e) (1) (v)) an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing PHI for any purpose other than the litigation or proceeding for which such information was requested; or requires the return to the covered entity or destruction of the PHI, including copies made, at the end of the litigation or proceeding.

### **PROCEDURES**

1. Disclosures of Protected Health Information (PHI) **without** the authorization of the individual may be made according to the above policies.
2. When releasing PHI to a law enforcement entity/officer the City's Human Resources staff will verify that the person is a valid law enforcement entity/officer by requesting the agency identification badge, official credentials, and/or proof of government status.

Helpful guidance from: [http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/final\\_hipaa\\_guide\\_law\\_enforcement.pdf](http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf) notes: The Plan may disclose PHI to law enforcement with the individual's signed HIPAA authorization. The Plan may disclose PHI to law enforcement without the individual's signed HIPAA authorization in certain incidents, including:

- a. To report PHI to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- b. To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the premises of the covered entity.
- c. To alert law enforcement to the death of the individual when there is a suspicion that death resulted from criminal conduct.
- d. When responding to an off-site medical emergency, as necessary to alert law enforcement to criminal activity.
- e. To report PHI to law enforcement when required by law to do so (such as reporting gunshots or stab wounds).
- f. To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement



- c. If it is mandatory, a covered entity may disclose the protected health information pursuant to § 164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law.
- d. If the disclosure is not required (but only permitted) by the Federal law, the covered entity must determine if the disclosure comes within one of the other permissible disclosures. If the disclosure does not come within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it.
- e. If another Federal law prohibits a covered entity from using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other Federal law and not use or disclose the information.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.512.
- The Plan's Privacy Officer.

**City of Stockton**

**Request for Access to Protected Health Information (PHI) Without Authorization  
from an Individual**

---

---

Name of Individual for Whom PHI is Requested: \_\_\_\_\_

Print Name of Party Requesting the PHI: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

I, \_\_\_\_\_ am requesting that I be allowed to inspect and copy the following PHI for the above  
named individual: *(List PHI requested)*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Reason for Request of PHI: \_\_\_\_\_

\_\_\_\_\_

Signature of Individual Requesting Access to PHI: \_\_\_\_\_

Date: \_\_\_\_\_

***Attach copy of identification of the individual requesting the PHI to this form along with any other  
documentation of the reason for PHI disclosure. (e.g. subpoena, court order, etc.)***

<p><i>Once completed, please return this form to the:</i> <b>City of Stockton Deputy Director of Human Resources – Risk &amp; Benefits</b> 400 E. Main Street., 3<sup>rd</sup> Floor Stockton CA, 95202 Telephone: 209-937-8233 Confidential fax #: 209-937-5702</p>
--

## HIPAA PRIVACY POLICY AND PROCEDURE ON RECORD RETENTION AND DESTRUCTION

---

---

### POLICY STATEMENT

*Note: This policy specifically focuses on the record retention period requirements specific to the administration of the Plan and, as such, is not meant as an exhaustive list of all record retention requirements to which the Plan and/or an Employer may be subject under Federal laws other than the Employee Retirement Income Security Act of 1974 (ERISA) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Specifically, the Plan will have general recordkeeping requirements under the Internal Revenue Code as a taxpayer and under various other Federal laws as an employer.*

While the Plan acknowledges that there are State and Federal record retention requirements for specific types of information (i.e., financial, personnel, trade/service mark, OSHA, Fair Labor Standards, IRS, Civil Rights Act and Equal Pay Act, etc.) this policy and procedure is drafted to provide guidance to this Plan on record retention in order to comply with the HIPAA Privacy regulations.

This policy and procedure is adopted pursuant to Sections 164.530(j), 164.528, 160.310(a) and various other sections and requirements of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan acknowledges that it must:

- a. Maintain the policies and procedures in written or electronic form; and
- b. If a communication, action, activity, or designation is required by the Privacy regulation such communication, action, activity, or designation documentation must be maintained in writing or electronic copy.

In compliance with the regulations, **the Plan must retain required documentation for the later of six years from the date of its creation or the date when it last was in effect.**

The Plan must keep such records and submit such compliance reports, in such time and manner and containing such information, as the HHS Secretary may determine to be necessary to enable the Secretary to ascertain whether the Plan has complied or is complying with the applicable requirements of the applicable standards, requirements, and implementation of the Privacy regulations.

In compliance with 164.528 the Plan will retain proof of its accounting of disclosures of protected health information for the six years prior to the date on which the accounting was requested, except for disclosures:

- To carry out treatment, payment and health care operations as provided in § 164.506;
- To individuals of protected health information about them as provided in § 164.502;
- Pursuant to an authorization as provided in § 164.508 (however signed authorizations will be retained);
- To persons involved in the individual's care or other notification purposes as provided in § 164.510;
- For national security or intelligence purposes as provided in § 164.512(k)(2);
- To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or
- That occurred prior to the compliance date for this Plan as covered entity.

#### **Record Retention Period Policy:**

The Plan will comply with HIPAA's privacy rules that require that any required documentation must be retained (either in written or electronic form) **for the later of six years from the date it was created or the date it was last in effect.**

**Provide records and compliance reports.** A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

**Cooperate with complaint investigations and compliance reviews.** A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

### Permit access to information.

1. A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.
2. If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.
3. Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

### KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Electronic media** means:
  - a. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and
  - b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
- **Record** means an item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for this Plan as a covered entity. Record **does not** include:
  - a. Education records relating to a student or as maintained by an educational agency or institution or by a person acting for such agency or institution covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g and what is not an education record at 20 U.S.C. 1232g(a)(4)(B)(iv);
  - b. Employment records held by this Plan (a covered entity) in its role as employer. Employment records (while not officially defined by the Privacy Regulations), under this policy and procedure means information needed by this employer to facilitate FMLA requests, sick leave requests, drug screening programs, fitness-for-duty exams, OSHA requirements and other similar programs. Health information that is received by this employer in its employment capacity is not protected health information (PHI) and therefore not a record as defined in this policy.

### PROCEDURES

#### Record Retention Procedures

A. Types of Documents and their associated record retention periods are described in the chart below:

Type of Record Document	Retention Period
<b>Policies and procedures related to HIPAA Privacy</b> including revisions and policies and procedures on PHI uses and disclosures.	Current year plus six prior years from the date when the policy or procedure was last in effect.
<b>HIPAA Privacy policies and procedures</b> , including protocols for PHI use, routine disclosures and requests	Current year plus six prior years from the date when the policy or procedure was last in effect.
<b>Signed authorizations, revocation authorization</b>	Indefinitely for a valid authorization form. Six years from the date the revocation of an authorization is in place

Type of Record Document	Retention Period
<b>Privacy Notice and revised Notices</b>	Six years
<b>Documentation regarding the following individual rights:</b> (1) designated record sets subject to inspection and copying by an individual, and the name or title of the persons or offices responsible for receiving and processing the requests; (2) the name or title of the persons or offices responsible for receiving and processing individual requests for PHI amendment; (3) documentation of any agreed-upon restrictions on the PHI use or disclosure requested by an individual; and (4) documentation of any amendments/corrected PHI or any denial of request to amend PHI or individual's statement of disagreement.	Six years
<b>Records of PHI disclosure for non-TPO purposes.</b>	Six years
<b>Individual complaints and the outcome of the complaint including documentation related to possible or actual breaches of unsecured PHI, investigative reports, risk assessments and notices.</b>	Six years after complaint, incident or breach
<b>Records of sanctions imposed on employees, agents, subcontractors or business associates.</b>	Six years after sanction
<b>Records on PHI use and disclosure for research purposes, as allowed without authorization under the privacy rules.</b>	Six years after completion of research project.
<b>Plan Document(s)/Summary Plan Description and HIPAA Privacy text amendments</b>	Indefinitely
<b>Business associate contracts and amendments to contracts</b>	Six years after contract expiration or termination
<b>Written Certification Statement(s)</b>	Six years
<b>Employee training manuals and procedures</b> <i>(recommended but not required)</i>	Six years

Upon expiration of the designated record retention period, documents will be destroyed in a manner consistent with the Plan's procedure on record destruction.

- The Plan will retain records to enable the Secretary of Health and Human Services (HHS) to ascertain/audit whether the Plan or the Plan's business associate has complied or is complying with HIPAA regulations.
- The **death of an individual**, will not cause the duration of record retention under this policy and procedure to change in any manner for **50 years after the person's death**. Individually identifiable health information of an individual who died more than 50 years ago is no longer PHI that must be protected by the privacy rule.

B. The following chart outlines the manner in which records will be retained:

<b>Form of Record Retention</b>	
<b>Hard Copy Records</b>	While no particular form of record retention is mandated; this Plan will retain records of sufficient detail to provide the basic information and data by which the document may be verified, explained, clarified and/or checked for accuracy and completeness.
<b>Electronic Records</b> (e.g. images, computer disc, microfilm, CD, tape, flash drive, etc.)	<p><b><u>This Plan will use the following guidelines on electronic recordkeeping (according to the Department of Labor for ERISA plans) until HIPAA rules for electronic recordkeeping have been finalized.</u></b></p> <ol style="list-style-type: none"> <li>1. The recordkeeping system reasonably ensures the integrity, accuracy, authenticity, and reliability of electronic records; and</li> <li>2. The electronic records are kept in a safe and accessible place, and may be readily inspected or examined; and</li> <li>3. The electronic records can be converted into paper copy; and</li> <li>4. There are adequate records management practices.</li> </ol> <ol style="list-style-type: none"> <li>a. Original paper records may be discarded at any time after they have been transferred to an electronic recordkeeping system, <b>except if</b> an electronic reproduction would not constitute a duplicate record.</li> <li>b. When upgrading or changing its data-processing capabilities the Plan will assure that electronic records can be converted or read to a compatible format.</li> </ol>

**C. Maintaining hard copy documents:**

- Documents will be stored for seven years onsite in the Plan’s City’s Human Resources department and then transported to the Plan’s secure offsite storage for the remaining years as outlined on the Record Retention period chart above.
- Long term storage of hard copy documents will be managed by the Privacy Officer using the services of a subcontracted offsite storage vendor.
- The Privacy Officer will oversee transport of PHI from the City’s Human Resources Department to the subcontracted offsite storage vendor. The Privacy Officer will assure that a Business Associate Agreement is in place with the offsite storage company since this Plan requires that PHI be transported to and from the City’s Human Resources department by the offsite vendor.
- Only those City’s Human Resources staff authorized by the Privacy Officer may request and retrieve PHI from the offsite storage company. The Privacy Officer will maintain a log of record retrieval activity.

**D. To ensure the integrity of stored electronic records, the Privacy Officer or designee will:**

- test the storage media prior to its being used for storing electronic records to verify that it is free from errors and defects.
- maintain the storage media in a temperature- and humidity-controlled environment.
- periodically read a sample of all storage media to identify any loss of data and any media likely to deteriorate, such as computer tapes, should be copied onto new media before deterioration is likely.

### **Record Destruction Procedures**

- For electronic media, only the Plan's Privacy Officer will authorize the destruction of the Plan's electronic media (such as CD, tapes, discs, USB data stick/flash drive, hard drives, etc.) **in accordance with instructions from the Plan's IT Director or HIPAA Security Officer.**
- Electronic media will be destroyed using the following methods: degaussing using a strong magnetic field to scramble the media, appropriate wiping program such as zeroization where zeroes or other symbols are written over the text, destruction such as shredding.
- For destruction of paper documents the City Clerk's Office will maintain a log of destruction due dates. Upon the due date or within 2 months after the due date the Privacy Officer or designee will assure the destruction of documents by shredding.

### **POLICY/PROCEDURE VIOLATION**

Refer to the policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.530(j), 164.528, 160.310(a).
- The Plan's Privacy Officer.

## **HIPAA PRIVACY POLICY AND PROCEDURE FOR USE AND DISCLOSURE OF PHI REQUIRING AN OPPORTUNITY FOR AN INDIVIDUAL TO AGREE OR OBJECT**

---

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.510(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), the Plan will follow the revised rules.

**The Plan may use or disclose protected health information (PHI), provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure,** in accordance with applicable requirements of this policy. The Plan may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure of PHI permitted by this policy.

#### **Uses and disclosures of PHI for involvement in the individual's care and notification purposes:**

The Plan may disclose to a family member, other relative, or a close personal friend of an individual, or to any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care. This disclosure can only be made according to the Plan's Procedure described below.

The Plan may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with this policy.

In addition, the Plan may disclose a deceased individual's PHI to family member, other relative or close personal friend of the deceased individual or any other person previously identified by the deceased individual to the Plan if the disclosure is directly relevant to such person's involvement with the deceased individual's care or payment related to the deceased individual's health care, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the Plan. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the privacy rules.

#### **Uses and disclosures with the individual present.**

If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, the Plan may use or disclose the PHI if it:

- Obtains the individual's agreement;
- Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

#### **Limited uses and disclosures when the individual is not present.**

If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. The Plan may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

If the individual is deceased, a covered entity may disclose to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

## **Use and disclosures for disaster relief purposes.**

The Plan may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosure of PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. These requirements apply to such uses and disclosure to the extent that the Plan, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

## **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

## **PROCEDURES**

### **1. Use or Disclosure with the Individual Present**

If an individual is present for, or otherwise available prior to a use or disclosure to those involved in an individual's care or for notification purposes, and the individual has the capacity to make health care decisions, the Plan may use or disclose PHI if the Plan:

- a. Obtains the individual's agreement (either orally or in writing);
- b. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- c. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

### **2. Limited Uses and Disclosures When the Individual is not Present**

If an individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. The Plan may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interests in allowing a person to act on behalf of the individual in obtaining PHI on their behalf to assist an individual in their care or payment for their care.

If the individual is deceased, a covered entity may disclose to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the privacy rules.

### **3. Use and Disclosure for Disaster Relief Purposes**

The Plan may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted to notify or assist in notifying persons involved in an individual's care. Disclosures to these entities must be made according to section 1 and 2 (*noted above*) where the Plan Office determines, in the exercise of its professional judgment that the requirements in section 1 and 2 do not interfere with the ability to respond to an emergency situation.

### **4. Documentation**

All written agreements to allow disclosure or written objections to the disclosure must be kept according to the Plan's Record Retention Policy.

### **5. General Purpose**

The general purpose of this policy is to allow disclosure in those limited instances where disclosure of protected information to next-of-kin (or to those with a close relationship to an individual) is necessary, or it is needed in order to locate next-of-kin or other individuals involved in their care. This policy will also allow disclosure of PHI to disaster relief organizations under certain circumstances. Disclosures made under this policy and procedure are not subject to the Plan's verification policy.

## 6. Exceptions

This policy and procedure will not apply to disclosures to individuals who are personal representatives in accordance with the Plan's Recognition of Personal Representative Policy & Procedure.

**This policy and procedure does not apply to disclosure made to avert an imminent threat to health or safety, as described in the Plan's Policy Regarding the Disclosure for Public Health, Law Enforcement, or Legal Process.**

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.510
- The Plan's Privacy Officer

## HIPAA PRIVACY POLICY AND PROCEDURE ON COMPLAINTS

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.530(d), 164.306, 164.310(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

In compliance with section 530(d), the Plan will provide a process for individuals to make complaints concerning the Plan's Privacy policies and procedures or the requirements of the Privacy regulations. Further, the Plan will document complaints and the disposition of complaints.

Under this Plan, the Privacy Officer is designated as the individual responsible for overseeing the complaint process. The Plan accepts and will investigate complaints of violations of the Plan's privacy policies and procedures from covered individuals as well as complaints from Plan staff. The Privacy Officer will determine:

- Whether there has been a violation of the Plan's privacy policies and procedures,
- The seriousness and effect of the violation, and
- Any corrective action that may be taken.

The Plan will document all complaints received and the outcome of the investigation.

### **Complaints to the Secretary of HHS:**

In compliance with section 164.306, the Plan acknowledges that a person who believes the Plan or its Business Associate is not complying with the applicable requirements of the standards, requirements, and implementation specifications of the Privacy regulations may file a complaint with the Secretary of HHS.

Complaints under this section must meet the following requirements:

- A complaint must be filed in writing, either on paper or electronically;
- A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable standards, requirements, and implementation specifications of the Privacy regulation;
- A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, (unless this time limit is waived by the Secretary for good cause shown);
- The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register and
- The Secretary may investigate complaints and such investigation may include a review of the pertinent policies, procedures, or practices of the Plan and of the circumstances regarding any alleged acts or omissions concerning compliance.

### **Investigation of Complaints by the Secretary of HHS:**

In compliance with section 164.310(b) the Plan will cooperate with the Secretary of the Department of Health and Human Services (HHS), if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the Plan to determine whether it is complying with the applicable standards, requirements, and implementation specifications of the Privacy regulation.

The Secretary will investigate any complaint filed under this section 160.306 when a preliminary review of the facts indicates a possible violation due to willful neglect.

- The Secretary may investigate any other complaint filed under this section.
- An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.
- At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

In accordance with section 160.308, the Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

## **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

## **PROCEDURES**

1. **Filing a Complaint:** The Plan will accept written complaints from covered individuals and employees. Complaints to the Plan must be in writing, preferably on the Plan's Privacy Complaint Form. Complaints must contain:
  - a. The date of the complaint;
  - b. The date of the alleged violation or other action that is the subject of the complaint;
  - c. The name of the person against whom the complaint is made;
  - d. A detailed description of the complaint; and
  - e. The name and signature of the person filing the complaint.
2. When the Plan receives oral complaints from covered individuals, the Plan will inform the individual that complaints must be in writing and they will provide that individual with a Plan Complaint Form to complete and return to the Plan.
3. The Plan will date-stamp the complaint when it is received.
4. The Plan will forward written complaints to the Privacy Officer for review. The Privacy Officer will also review the policy/procedure on "**Notification in the Case of Breach.**"
5. **Complaint Research:** The Privacy Officer will investigate all complaints within 60 days of the date the complaint is filed with the Plan, including taking any or all of the steps noted below:
  - a. Question the covered individual or employee making the complaint, if necessary;
  - b. Question the party alleged to have violated the privacy policies and procedures;
  - c. Consider any documents, evidence or testimony offered on behalf of the party alleged to have violated the Plan's privacy policies and procedures;
  - d. Determine whether there has been a violation of the Plan's privacy policies and procedures;
  - e. Determine whether any corrective action is necessary as a result of the complaint;
  - f. Implement or oversee the implementation of any corrective measures necessary as a result of the complaint;
  - g. Document any corrective measures taken;
  - h. When appropriate, the Privacy Officer may inform the person who filed the complaint of the Plan's actions to remedy such issues in the future; or
  - i. The Privacy Officer will keep a record of the complaint investigation, including the complaint and the Plan's findings, to ensure consistency of determinations and corrective measures for similar violations. The Privacy Officer may choose to also keep a complaint log if there are numerous written complaints accumulated.
6. If a complaint is lodged against the Privacy Officer the complaint will be investigated by the City's Director of Human Resources.
7. **Record Retention:** The Plan will retain written records related to a complaint and any corrective actions in accordance with the Plan's Record Retention policy.
8. The Privacy Officer will coordinate any and all complaints in which the Secretary of HHS is involved with the Plan.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR 164.530(d), 164.306, 164.310(b).
- The Plan's Privacy Officer.
- See also the policy/procedure in this manual on "Notification in Case of Breach."

**City of Stockton**  
**Privacy Complaint Form**

Name of Person Filing the Complaint: \_\_\_\_\_

Today's Date: \_\_\_\_\_

Date of Alleged Violation: \_\_\_\_\_

Name of Individual perceived to have violated the privacy policies and procedures:  
\_\_\_\_\_

Provide a detailed description of the complaint:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I am completing this complaint form regarding the Plan's practices, policies, procedures or compliance under the privacy standards of the Health Insurance Portability and Accountability Act (HIPAA). I understand that this complaint will be submitted to the Plan's Privacy Officer. I understand that although the Plan reviews and makes determinations regarding every complaint received, the Plan does not respond to every complaint in writing. I understand that the Plan cannot retaliate against an employee for filing a complaint/report about a violation of privacy rules.

Signature of Person Filing the Complaint: \_\_\_\_\_

For internal Plan use only:            Date complaint reviewed by Privacy Officer: \_\_\_\_\_

Assessment of the Complaint (*use back of form if more space needed*):  
\_\_\_\_\_  
\_\_\_\_\_

*Outline Privacy Officer's Action Taken:*

Date	Investigation and Action Taken

Sanction Applied? \_\_\_\_\_

Privacy Officer Signature: \_\_\_\_\_ Date of Complaint Resolution: \_\_\_\_\_, 20\_\_\_\_

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233      Confidential fax #: 209-937-5702

## HIPAA PRIVACY POLICY AND PROCEDURE FOR DE-IDENTIFICATION AND RE-IDENTIFICATION OF PHI

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514 and 502(d) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012. If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

**De-identification:** The Plan may disclose health information that it has determined does not contain individually identifiable information by removing the 18 identifiers from the information it uses or obtains. To determine that information it discloses does not contain individually identifiable health information it must follow one of the following methods.

- a. A person with knowledge of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that:
  - the risk is very small that the information disclosed could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information; and
  - applies methods to mitigate risk; and
  - The Plan documents the methods and the result of the analysis that justify this determination.
  - If this procedure is used, the expert will comply with the guidance set forth in the Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012.

**or, the safe harbor method:**

- b. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and the Plan does not have knowledge that the information provided could be used alone or in combination with other information to identify an individual who is a subject of the information:
  - (1) **Names;**
  - (2) All **geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip codes.**
    - The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census, (<http://www.census.gov/>) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people.
    - If the geographic units that make up the initial three digits of a zip code contain 20,000 or fewer people, the first three digits must be changed to 000.
    - Utilizing Census 2000 data, zip codes with the following initial three digits must have the zip code changed to 000: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, 893.
  - (3) **All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89** and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    - For example, de-identified information could not include the day and month of a medical procedure or event (i.e., 1/1/2009), but it may include only the year (i.e.2009).
    - Age may be included in de-identified information except that **age over 89 must be indicated as “90 or above”** whether the actual age is stated or implied (i.e., if the birth year is 1910 and treatment is provided in 2010, the birth year must be reported as “on or before 1920.”
  - (4) **Telephone numbers;**
  - (5) **Fax numbers;**

- (6) **Electronic mail (e-mail) addresses;**
- (7) **Social security numbers (SS#);**
- (8) **Medical record numbers;**
- (9) **Health plan beneficiary numbers;**
- (10) **Account numbers;**
- (11) **Certificate/license numbers;**
- (12) **Vehicle identifiers and serial numbers, including license plate numbers;**
- (13) **Device identifiers and serial numbers;**
- (14) **Web Universal Resource Locators (URLs);**
- (15) **Internet Protocol (IP) address numbers;**
- (16) **Biometric identifiers, including finger and voice prints;**
- (17) **Full face photographic images and any comparable images; and**
- (18) Any other unique identifying number, characteristic, or code, except as permitted for re-identification of the data as described below. For example, a unique identifier could be that the individual is the “current President of the University” or a clinical trial number.

**Parts or derivatives of any of the above listed identifiers may not be included in de-identified information. For example, de-identified information may not include the last four digits of the individual’s social security number or the individual’s initials.**

**Re-identification:** The Plan may assign a code or other means of record identification to allow information de-identified to be re-identified by the Plan provided that:

- a. The code or other means of record identification is not derived from or related to the individual;
- b. The code or other means cannot be translated so as to identify the individual;
- c. The Plan does not use or release the code or other means of record identification for any other purpose; and
- d. The Plan does not disclose the mechanism for re-identification.

## **KEY DEFINITIONS**

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **De-identified** means health information that does not identify an individual and which the Plan believes there is no reasonable basis that the information can be identified. De-identified information is not individually identifiable health information.
- **Re-identified** means assignment of a code or other means of record identification to allow the identification of the original identity that was de-identified.

## **PROCEDURES**

### **1. DE-IDENTIFICATION**

De-identified information is PHI stripped of identifiers so that the information is no longer required to be protected by the Privacy Rule. The Privacy Rule provides for two de-identification methods: (a) formal determination by a qualified expert or (b) removal of 18 specified identifiers (the safe harbor method). **This Plan has elected to follow method “b” (as described above under the Policy Statement) and all 18 identifiers described above will be removed in order for the Plan to de-identify PHI.**

Regarding the safe harbor method, the guidance clarifies the following:

- De-identified information cannot include parts or derivatives of identifiers, such as the last four digits of a Social Security number or a patient’s initials.
- Only the initial three digits of a zip code may be included in de-identified information, except no elements of a zip code may be included if 20,000 or fewer residents live in that zip code (the guidance includes a list of zip codes with fewer than 20,000 residents).

- The names of group health plan employees or health care providers may — but are not required to — be included in de-identified information.

In addition, the guidance on de-identified health information explains which elements of dates may be included in de-identified information:

- In particular, the year (*i.e.*, 2012) of a medical procedure or event may be included, but not the day and month (*i.e.*, 1/1/2012).
- Age also may be stated in de-identified information, except that ages over 89 must be indicated as “90 or above,” whether the actual age is stated or implied (*i.e.*, if the birth year is 1910 and treatment is provided in 2012, the birth year must be reported as “on or before 1920”).
- **Note that if claim appeals are presented by the Plan to the Plan Sponsor for appeal determination, documents should be properly de-identified. If more information is needed to be presented in order to make the claim determination, the Plan will obtain the patient’s written authorization.**
- There may be other unique identifiers (beyond the 18 listed) that also have to be removed to de-identify the information. Examples include the fact that an individual is the “current President of State University,” or a clinical trial identifying number.
- Even if all of the 18 identifiers are removed, protected health information still is not de-identified if the plan or business associate has actual (clear and direct) knowledge that there remains information that can be used alone or in combination with other information to identify an individual who is the subject of the information.
- Plan staff should consult with the Privacy Officer for assistance in determining if PHI has been thoroughly de-identified.

**2. RE-IDENTIFICATION:** The Plan will assign a code or other means of record identification to allow de-identified information to be re-identified by the Plan, in accordance with the Policy Statement described above.

- The Privacy Officer will retain documentation of re-identification code methods for six years.
- Individuals who are unsure on how to de-identify and re-identify information should seek clarification from the Privacy Officer.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.514, 164.502(d)
- The Plan’s Privacy Officer.

# HIPAA PRIVACY POLICY AND PROCEDURE ON SANCTIONS FOR VIOLATION OF PRIVACY RULES

---

---

## POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(e) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Plan or the requirements of the HIPAA Privacy regulations. The Plan must document the sanctions that are applied, if any.

An employee of the Plan who is responsible for handling Protected Health Information (PHI) of covered individuals will be sanctioned for violating the HIPAA privacy rules and the privacy policies and procedures adopted by the Plan. However, the Plan will not impose sanctions on whistleblowers or members of its workforce who are crime victims as those terms are defined elsewhere in these policies and procedures.

The Privacy Officer will determine whether there has been a violation of the privacy rules, the seriousness and effect of the violation and the sanction to be imposed on the covered individual.

The Privacy Officer has discretion to determine appropriate sanctions for violation of the privacy rules. Sanctions will include disciplinary action up to and including dismissal of an employee.

Sanctions will not be imposed for disclosure of PHI that meets the conditions set out in sections 164.530(g)(2) of the privacy rules regarding whistleblower protections.

## KEY DEFINITIONS

Under this Plan, **sanction refers** to the ramifications on an individual for breaking Plan policies related to HIPAA Privacy and Security. For assistance understanding common terms used in this manual, refer to the cover page.

## PROCEDURES

1. All Plan employees are required to report any perceived violations of the Plan's privacy policies and procedures to the Privacy Officer. Reports may be made orally (with written follow-up) or in writing to the Privacy Officer.
2. Reports are to be documented on the Plan's form titled "Privacy Complaint Form" (see copy behind the Policy on Complaints).
3. Conduct of the Plan's workforce that could result in disciplinary action under these sanction procedures includes but is not limited to:
  - Accessing a person's PHI out of curiosity or for a purpose beyond the scope of treatment, payment or health care operations, or in a manner not in compliance with an authorization form;
  - Discussing PHI in a public area or outside the designated group health plan area;
  - Removing PHI from the designated group health plan area (such as with paper or electronic including laptop, PDA, USB storage device, etc.) without appropriate authorization and security;
  - Attempting to gain unauthorized access to PHI by any means;
  - Failing to send PHI electronically in a safe/secure manner;
  - Failing to logoff or, leave a computer on and unsecured;
  - Copying or compiling PHI with the intent to sell, or use for personal or financial purposes; or
  - Failing to follow the HIPAA Privacy or Security policies and procedures of the Plan.
4. The Privacy Officer will (in conjunction with the Plan's Security Officer as needed):
  - Investigate (and document the investigation) of the alleged violation of the privacy rules (while maintaining confidentiality);
  - Question the employee or person reporting the perceived violation;

- Question the employee or person who is alleged to have violated the privacy rules;
  - Consider (and preserve) any evidence or testimony accompanying the report of violation or submitted on behalf of the employee alleged to have violated the privacy rules;
  - Determine whether there has been a violation of the privacy rules; and
  - Make and keep a record of the investigation.
5. As pertains to an employee's violation of the Plan's HIPAA Privacy policies and procedures, the Privacy Officer will assess the gravity of the violation of the privacy rules, and apply the appropriate sanction on the employee. Sanctions will be applied consistently.
  6. The Privacy Officer or Plan Administrator (in conjunction with the Plan's Security Officer as needed) has discretion to determine appropriate sanctions on employees and will consider:
    - The exposure of PHI that resulted from the violation;
    - Intent: whether the violation is accidental or egregious/intentional;
    - Pattern: whether it is a first-time violation or a repeated violation; and
    - Issues will be evaluated on the basis of the nature and extent of the infraction and the seriousness of the PHI disclosure, the extent of harm as a result of the disclosure and whether or not the issue was intentional or accidental.
  7. Sanctions on Plan employees can include, but are not limited to any of the following:
    - verbal reprimand;
    - written reprimand;
    - required remedial comprehensive HIPAA training;
    - possible escalation of the violation or incident to Human Resources, legal counsel or outside authorities;
    - requirement to transfer to work in a non-Plan worksite;
    - suspension from duty for a certain period of time without pay;
    - administrative leave with pay pending outcome of the PHI breach;
    - recommendation of termination of employment; or
    - civil and criminal penalties.
  8. The Privacy Officer will make and keep a record of the violation and the sanctions imposed to ensure consistency of sanctions for similar violations. All reporting will be kept confidential.
  9. The Privacy Office will determine how to prevent (mitigate) this situation from occurring again in the future.
  10. Sanctions will not be imposed for disclosures of protected health information that meet the conditions described in sections 164.530(g)(2) and 164.502(j) of the privacy rule regarding whistleblower protections.
  11. Documentation of complaints, investigation, correspondence and sanctions will be kept in accordance with the Plan's policy on Record Retention.
  12. There will be no retaliation against employees for reporting a HIPAA privacy violation to the Plan.
  13. The Plan will work with legal counsel to determine if there are any collective bargaining issues (CBA) issues that may exist before adopting any new disciplinary procedures.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Breach.

## **ADDITIONAL RESOURCES**

- 45 CFR Section 164.530(e)
- The Plan's Privacy Officer

## HIPAA PRIVACY POLICY AND PROCEDURE FOR TRAINING

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan must train all members of its workforce on the policies and procedures with respect to protected health information (PHI) required by the HIPAA Privacy regulation, as necessary and appropriate for the members of the workforce to carry out their function within the Plan. This training must meet the following requirements:

- a. To each member of the Plan's workforce by no later than the compliance date for the Plan (April 14, 2003);
- b. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the Plan's workforce; and
- c. To each member of the Plan's workforce whose functions are affected by a material change in the policies or procedures required by the HIPAA Privacy Regulation or the procedures of this Plan, within a reasonable period of time after the material change becomes effective.
- d. The Plan must document that the training, as described above, has been provided.

Therefore it is the policy of the Plan to train the Plan's workforce, including all personnel who administer the group health plan, on all Plan policies and procedures concerning the use or disclosure of protected health information implemented for compliance with the Privacy requirements under HIPAA. The Plan will retrain personnel as necessary.

### KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Workforce** means employees, volunteers, trainees and other persons whose conduct, in the performance of work for the Plan, is under the direct control of the Plan, whether or not they are paid by the Plan.

### PROCEDURES

1. The Privacy Officer will arrange for all training and ensure that appropriate workforce personnel are trained on HIPAA Privacy, security and breach regulations.
2. **Timing of Training:**
  - a. The Plan will provide training to all of the personnel that work with and for the Plan no later than April 14, 2003.
  - b. After April 14, 2003, each new employee of the Plan will be trained within a reasonable time after they join the Plan.
  - c. When there is a material change in the Plan's policies, procedures or forms, each employee of the Plan will be trained on the new information. This training will take place within a reasonable time after the material change becomes effective.
  - d. The Plan will re-train Plan personnel at least annually, as necessary.
  - e. The Plan will train individuals who work in or with the administration of the Plan (such as temporary employees, independent contractors, volunteers, trainees and employees floating from other departments to help in the Plan administration area) as necessary based on their assignment within the Plan. The Plan will have all these types of individuals sign a confidentiality agreement within a reasonable time following their start date as a way to reinforce the need to maintain required privacy.
3. **Manner of Training:**
  - a. After April 14, 2003, new Plan employees will attend an instructional session conducted by the Plan's Privacy Officer or the City's Supervising Human Resources Analyst – Benefits or designee, discussing the Plan's privacy policies and procedures. HR Management may, in addition to or, as a substitute for this training, arrange for Plan employees to attend training on HIPAA privacy rules conducted by an entity outside of the Plan office with expertise in HIPAA's privacy rules. This training may be live, on the phone, or via the Internet.

- b. Plan training will include a discussion of prohibited uses and disclosures of PHI as well as any sanctions that may be imposed against personnel who violate the Plan's privacy policies and procedures and the contact information for the Privacy Officer.
- c. As part of this initial training, Plan employees will review the Plan's written privacy policies and procedures as well as the Plan's HIPAA Privacy Notice. Plan employees will be informed where they can access and review a copy of the Plan's HIPAA Privacy Notice.

**4. Documentation:** Because the Plan is required to document training, the following steps will occur:

- a. Each employee of the Plan will certify in writing that they have completed the initial privacy training.
- b. Each employee of the Plan will certify in writing their participation in subsequent training/retraining.
- c. Employees will certify in writing that they have completed training by signing an attendance sheet. This attendance sheet will be completed and returned to the Privacy Officer after each training session.
- d. The Privacy Officer will retain a copy of the training material provided with each staff training along with the applicable date the training was performed and their signature on the attendance list as proof of training attendance.
- e. The Plan may, but is not required to, have plan employees complete the Training Certification and Confidentiality Agreement form in this manual.

**5. Composition of HIPAA Training for Plan Employees**

- a. Initial new employee training will include the following components (many of these training topics are found in this Policy and Procedure Manual):
  - Overview of the HIPAA Administrative Simplification regulation
  - Discussion on which employee benefits are regulated and not regulated by HIPAA
  - Understanding who is a Covered Entity and why is that important
  - Purpose of HIPAA Privacy regulations
  - Understanding of Individually Identifiable Health Information (IIHI) versus Protected Health Information (PHI)
  - What is PHI and how to de-identify information
  - Discussion of what/who comprises the group health plan
  - When is enrollment information considered to be PHI
  - Discussion about employment records that are not regulated by HIPAA
  - That employers may not use PHI for discipline, hiring, firing, placement, promotion/demotion, etc.
  - Understanding of Minimum Necessary
  - Four primary ways the group health plan can release PHI without an individual's permission
  - Personal representatives and Authorization forms
  - The Plan's verification of identity policy/procedures
  - Who are the Plan's Business Associates, BA contracts and the relationship of the BA to the covered entity
  - How documentation and forms will be maintained/destroyed in the Plan (record retention/destruction)
  - The HIPAA Privacy Notice: who gets it, when and how to distribute it, what it says, etc.
  - Individual rights about PHI: to amend, copy, access, transmit confidentially, accounting of disclosures
  - How to handle complaints about PHI
  - Safeguarding PHI in the Plan (oral, paper and electronic PHI)
  - The role of, location and usefulness of the Plans' Privacy Policy/Procedure manual(s) and necessary forms
  - The role of and how to contact the Privacy Officer (and any designees)
  - Penalties/sanctions for violation of the Plan's policies/procedures
  - What is electronic media

- Where is electronic PHI in a group health plan
- General HIPAA Security requirements
- Administrative, Physical, Technical safeguards plus Operational and Policies/Procedures for ePHI; the required Risk Analysis/Risk Assessment
- The role of email, zipping, encrypting, and scanning with ePHI
- Remote electronic users and portable devices
- Common security mistakes
- HIPAA Federal auditor requirements and findings
- What is a breach and what to do if there has been an incident
- Breach notification to individuals
- Online HHS breach reporting
- What's new since HIPAA Omnibus regulations released, such as PHI of deceased individuals, revised BA agreements needed, sale of PHI, limitation on use & disclosure of genetic information, revised Privacy notice, etc.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR 164.530(b)
- The Plan's Privacy Officer.

## City of Stockton Confidentiality Agreement

*To be completed in duplicate by employees or independent contractors of the City of Stockton group health plan. Original to be returned to the Privacy Officer within one week after signature.*

I \_\_\_\_\_ am an [employee] [temporary staff] in the **group health plan administration area of the Human Resources office of the City of Stockton**. I am aware that I may have access to individually identifiable health information (oral, written and electronic) and such should be treated in a professional and confidential manner. I agree that **I will not use or disclose** or cause to be disclosed any individually identifiable health information which I may have knowledge of at any time. Such information includes, but is not limited to individually identifiable information about health plan enrollment, eligibility, claims and appeals and external reviews, COBRA information, social security numbers, and information related to the self-funded medical plan options including outpatient prescription drug benefits and health reimbursement account (HRA), self-funded dental plan, self-funded vision plan, and Health Flexible Spending Accounts (FSA) to which I have access.

I certify that I have received information on the Plan's privacy policies as well as appropriate state and Federal laws concerning the confidentiality of individually identifiable health information, the improper release of such information and the alteration or destruction of such information. I have also been provided with a copy of the Plan's HIPAA Notice of Privacy Practices.

I will not use my personal camera cell phone (or my personal camera) to take pictures or videotapes or other electronic recording of any computer screen, person, item or document that is considered to be or contains HIPAA protected health information (PHI). I understand that if a picture or recording of PHI is needed, I will contact the Plan's Privacy Officer to discuss.

I am aware that any breach of confidentiality of this material or any abuse of my position, including, but not limited to, alteration of records, destruction of records or other similar acts, may constitute a basis for prompt disciplinary action or immediate termination of employment.

I understand that the Privacy Officer of the group health plan is:

<p><b>City of Stockton Deputy Director of Human Resources – Risk &amp; Benefits</b> 400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202 Telephone: 209-937-8233 Confidential fax #: 209-937-5702</p>
--

I have been shown the location of the Plan's privacy policies and procedures. I understand that if I have questions about the individually identifiable information that I receive or need to disclose, I am to contact the Privacy Officer.

Print Name of Employee \_\_\_\_\_

Signature of Employee \_\_\_\_\_ Date \_\_\_\_\_

Supervisor Signature \_\_\_\_\_ Date \_\_\_\_\_

CITY OF STOCKTON

**HIPAA Training Certification and Confidentiality Agreement Form**

To be completed in duplicate by employees or independent contractors of the City of Stockton. Original to be returned to the Privacy Officer within one week after signature.

I, \_\_\_\_\_, am (circle one), an Employee, Temporary Employee, or Independent Contractor of the **City of Stockton’s group health plan**, and hereby acknowledge and agree that it is the policy of the Plan to train the Plan’s workforce, including all Plan employee benefits office support personnel, on all Plan policies and procedures concerning the use or disclosure of protected health information implemented for compliance with the privacy requirements under HIPAA.

- I have attended the HIPAA Privacy training program performed or sponsored by the Plan, held on \_\_\_\_\_, 20\_\_\_. A copy of the presentation is on file with the Privacy Officer.
- I have received and reviewed a copy of the Plan’s Notice of Privacy Practices.
- I am aware of the location of the Plan’s HIPAA Privacy Policy and Procedure manual and that it is a resource for the Plan’s compliance with the Privacy regulation.
- I understand that if I have questions about the Plan’s Privacy Policies and Procedures I am to contact the Plan’s Privacy Officer.

<p align="center"><b>City of Stockton Deputy Director of Human Resources – Risk &amp; Benefits</b>  400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  Telephone: 209-937-8233 Confidential fax #: 209-937-5702</p>
---

- I agree to observe the Plan’s Privacy Policies and work in accordance with the Plan’s Privacy Procedures as I carry out the duties of my job.
- I agree to comply with any amendments to the HIPAA Privacy regulation the Department of Health and Human Services may make that the Plan may implement.
- I am aware of the prohibited uses and disclosures of Protected Health Information (PHI).
- I agree that Protected Health Information (PHI) is confidential and may not be used or disclosed to any individual or third-party not expressly permitted to receive Protected Health Information, either during **or after** my employment.
- I will not use my personal camera cell phone (or my personal camera) to take pictures or videotapes or other electronic recording of any computer screen, item or document that is considered to be or contains HIPAA protected health information (PHI). I understand that if a picture or recording of PHI is needed, I will contact the Plan’s Privacy Officer to discuss.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Address: \_\_\_\_\_

# HIPAA PRIVACY POLICY AND PROCEDURE FOR USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS (TPO)

---

## POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(a) and Section 164.506 of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

### General Rule:

The Plan (as a covered entity) or a business associate may not use or disclose PHI, except as permitted or required by HIPAA. The Plan is permitted to use or disclose PHI as follows:

1. **To the individual;**
2. For **treatment, payment, or health care operations (TPO)**, as permitted by and in compliance with the HIPAA rules on uses and disclosures of PHI to carry out TPO.
3. In accordance with a signed valid **authorization** (that complies with 164.508 as outlined in the Plan's policy on Use of Authorization.)
4. **When an authorization form is not required**, as permitted and in compliance with the HIPAA regulations outlined in the Plan's policy on the Use and Disclosure of PHI as Required by Law, etc. (164.512 and 164.514).

The Plan is required to disclose PHI to an individual or to the Secretary of the Department of Health and Human Services.

### Permitted Uses and Disclosures:

Except with respect to uses or disclosures that require an authorization (psychotherapy notes or marketing activities or sale of protected health information with remuneration), the Plan may use or disclose PHI for treatment, payment, or health care operations (TPO) without obtaining consent or an authorization form. Use and disclosure of PHI must be consistent with other applicable requirements of HIPAA (such as minimum necessary) as described in the policies and procedures of the Plan.

### Consent for Uses and Disclosures Permitted:

The Plan may obtain the consent of the individual to use or disclose PHI to carry out TPO. A voluntary consent document will not constitute valid permission to use or disclose PHI for a purpose that requires an authorization under the Privacy regulation (such as for psychotherapy notes or marketing or sale of protected health information with remuneration as described in Section 164.508 of the Privacy regulation). (See also the policies and procedures entitled Use of Authorization.)

Additionally a consent will not permit disclosure of PHI when another condition must be met for such use or disclosure to be permissible under HIPAA. *For example, the covered entity could not require a consent to release the entire medical record to resolve an emergency room claim dispute when another rule requires the covered entity to release the minimum necessary. The Privacy Rule does not affect informed consent for treatment that is required by state law.*

### Treatment, Payment, or Health Care Operations:

1. The Plan may use or disclose PHI for its own TPO uses. The Plan may disclose PHI for treatment activities of a health care provider.
2. The Plan may disclose PHI to another covered entity or health care provider for the payment of the entity that receives the information.
3. The Plan may disclose PHI to another covered entity (such as another group health plan, health care provider or clearinghouse) for health care operations activities of the covered entity that receives the information, if the Plan and the other covered entity have or have a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the purpose of:
  - Conducting quality assessment and improvement activities including patient safety activities;
  - Reviewing the competence or qualifications of health care professionals, evaluating performance, conducting training programs, accreditation, certification, licensing, or credentialing activities; or
  - Health care fraud and abuse detection or compliance.

4. A Plan that participates in an organized health care arrangement (this term is defined below) may disclose PHI about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

**Covered entity** means a:

- health plan;
- health care clearinghouse; or
- health care provider who transmits any health information in electronic form in connection with a transaction covered by the transaction standards in 45 C.F.R. Part 162.

**Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

**Payment** means:

1. The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
2. The activities related to the individual to whom health care is provided and include, but are not limited to:
  - a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
  - b) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - d) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  - e) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
  - f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    - Name and address;
    - Date of birth;
    - Social security number;
    - Payment history;
    - Account number; and
    - Name and address of the health care provider and/or health plan.

**Health care operations** mean any of the following activities of the Plan to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g)

are met, if applicable (§ 164.514(g) says that if a health plan receives protected **health** information for the purpose of underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law);

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the Plan, including, but not limited to:
  - b) Management activities relating to implementation of and compliance with the requirements of HIPAA;
  - c) Customer service, including the provision of data analyses for policyholders, Plan Sponsors, or other customers, provided that PHI is not disclosed to such policy holder, Plan Sponsor, or customer;
  - d) Resolution of internal grievances;
  - e) The sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
  - f) Creating de-identified health information, complying with minimum necessary rules, limited data sets, fundraising, underwriting and verification requirements of HIPAA for the benefit of the Plan.

**Organized health care arrangement means:**

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint activities that include at least one of the following:
  - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
  - Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
  - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk
3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plans each of which are maintained by the same Plan Sponsor; or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

## PROCEDURES

In order to manage the health benefits provided by the Plan, the Plan's staff will follow these procedures when using PHI.

### The Plan may use or disclose PHI without an authorization:

1. **When disclosing PHI to the individual who is the subject of the PHI** (See also the Plan's policy on Verification of Identity).
2. For **treatment, payment, or health care operations (TPO)**, as defined in the Policy statement above. For example, the Plan will provide PHI to a health care provider or health plan to obtain or provide reimbursement for the provision of health care related to an individual covered under the Plan.
3. **When an authorization form is not required**, as permitted and in compliance with the HIPAA regulations outlined in the Plan's policy on the Use and Disclosure of PHI as Required by Law, etc. (164.512 and 164.514).
4. When using **interpreter services**, the Plan may use and disclose protected health information regarding an individual without an individual's authorization as a health care operation, in accordance with the Privacy Rule, in the following ways:
  - When the interpreter is a member of the Plan's workforce (i.e., a bilingual employee) as defined at 45 CFR 160.103; or
  - When a covered entity engages the services of a person or company who is not a Plan workforce member, to perform interpreter services on its behalf, the Plan will obtain a Business Associate agreement with that interpreter person or company. The Plan may disclose the minimum necessary PHI to the business associate to allow them to provide meaningful translation of information to a person with limited English proficiency.

However, if a person with limited English proficiency provides a family member or close personal friend to perform the translation services, the Plan will try to obtain the prior written authorization of the person with limited English proficiency to allow the Plan to disclose PHI. In these situations, that interpreter is not a business associate of the Plan.

5. The Plan may obtain enrollment forms/information (including online benefits enrollment information) from employees. The enrollment forms/information will be used to enroll individuals into their selected health benefit options and to provide eligibility and enrollment/disenrollment data to the appropriate insurance companies, vendors and Business Associates of the Plan involved in administering health benefits, and to the payroll department to take the appropriate paycheck deductions. Enrollment forms/information also will assist the Plan in determining and fulfilling its responsibility for coverage and provision of benefits under the health plan.

Benefits enrollment confirmation statements are not protected health information when these statements are created and distributed prior to the effective date of the group health plan coverage, nevertheless the Plan will take measures to distribute benefits enrollment confirmation statements in a manner that removes or de-identifies SSNs and hardcopy statements will be distributed in a sealed envelope or allow the employee to print the statement from an online benefits enrollment system.

6. PHI will be used and shared in order to determine eligibility or coverage.
7. The Plan will use PHI to adjudicate or subrogate health benefit claims, assess risk based on enrollee health status and demographic characteristics.
8. To coordinate billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing.
9. To review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.
10. To oversee utilization review activities, including precertification of services, concurrent, retrospective review and case management.
11. To conduct or arrange medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
12. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and Business management and general administrative activities of the Plan, including, but not limited to: Resolution of internal grievances; creating de-identified health information. Complying with minimum necessary rules, limited data sets, fundraising, underwriting and verification requirements of HIPAA for the benefit of the Plan.

13. When in doubt staff are to obtain a signed authorization form to disclose PHI. See also the policy and procedures on Use of Authorization.
14. The Privacy Officer will retain documentation in accordance with the Plan's Record Retention policy.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Minimum Necessary and the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.502 (a) and Section 164.506.
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR MITIGATION

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(f) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

In compliance with Section 164.530, the Plan will mitigate, to the extent practicable, any harmful effects known by the Plan of a use or disclosure of protected health information (PHI) in violation of the Plan's policies and procedures or HIPAA regulations by employees of the Plan or any business associate.

In order to mitigate harmful effects, the use or disclosure of PHI that violates the Plan's procedures and/or HIPAA must be known to the Plan. This means the Privacy Officer must have been informed of the violation by an individual, a member of the Plan's workforce, or a business associate. When mitigating harmful effects, the Plan will take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to an individual, and what steps can be taken to have a mitigating effect in that specific situation.

### KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Mitigate** means to lessen or remove negative impacts.

### PROCEDURES

1. The Privacy Officer will document any notice that a use or disclosure of protected health information (PHI) by an employee of the Plan or business associate is in violation of the Plan's policies and procedures or HIPAA regulations.
2. The Privacy Officer will promptly initiate an investigation. The Privacy Officer will also review the policy and procedure in this manual related to Breach. The Privacy Officer reserves the right to contact legal counsel for assistance.
3. The Privacy Officer will initiate a corrective action to attempt to prevent future similar disclosures.
4. If the PHI misuse involves an employee of the Plan, the Privacy Officer will reference the Plan's sanction policy for employee disciplinary action.
5. If the PHI misuse involves a Business Associate, the Privacy Officer will:
  - a. obtain a copy of the Plan's Business Associate contract;
  - b. discuss the issue with the Business Associate and follow up in writing to document the conversation;
  - c. ask the Business Associate for a corrective action plan; and
  - d. determine if the corrective action plan is appropriate and if not, work with the Business Associate to develop an acceptable corrective action plan.

The Plan reserves the right to terminate a Business Associate Agreement if a mutually acceptable corrective action cannot be reached or the Plan finds that the Business Associate continues to misuse PHI despite notice by the Plan.

6. The Privacy Officer will retain documentation of the mitigation issue, investigation and resolution in accordance with the Plan's record retention policy.

### POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions and/or Breach.

### ADDITIONAL RESOURCES

- 45 CFR, Section 164.530(f).
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE REGARDING ANTI-RETALIATION

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530 (g) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

In compliance with Section 164.530, the Plan will not take retaliatory action against any person who files a complaint with the Plan or with the Department of Health and Human Services. The Plan and its Business Associates will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for exercising their rights under the privacy rules or for filing or participating in filing a complaint under the complaint process established by the Plan or the Privacy regulations;
2. Any individual or other person for filing a complaint with the Secretary of the Department of Health and Human Services under subpart C of section 160 of the regulations;
3. Any individual or other person for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act (relating to HIPAA Administrative Simplification, beginning with 42 U.S.C. § 1320d); or
4. Any individual or other person for opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful and the manner of the opposition must be reasonable and not involve a disclosure of PHI in violation of HIPAA regulations. For example, an employee who discloses their own PHI to the media or a friend is not protected.

### KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

### PROCEDURES

1. If the Privacy Officer is notified of a **retaliatory action against an individual or other person the Privacy Officer will** seek out the source of the person/department taking retaliatory action and educate them on the HIPAA regulations that prevent such action.
2. The Privacy Officer may take other action as needed to adequately address the retaliatory action issue.
3. The Privacy Officer will retain documentation of the investigation of the retaliatory action in accordance with the Plan's record retention policy and procedures.

### POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

### ADDITIONAL RESOURCES

- 45 CFR Section 164.530 (g).
- The Plan's Privacy Officer.

## **HIPAA PRIVACY POLICY AND PROCEDURE DISCLOSURES OF PHI BY WHISTLEBLOWERS AND VICTIMS OF CRIME**

---

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.502(j) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

#### **Disclosures by whistleblowers:**

The Plan is not considered to have violated the requirements of the Privacy regulation if a member of its workforce or a business associate discloses PHI provided that:

- a) The workforce member or business associate believes in good faith that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Plan potentially endangers one or more patients, workers, or the public; and
- b) The disclosure is to:
  - i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plan; or
  - ii) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

#### **Disclosures by workforce members who are victims of a crime:**

A Plan is not considered to have violated the requirements of the Privacy regulation if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that:

- a) The PHI disclosed is about the suspected perpetrator of the criminal act; and
- b) The PHI disclosed is limited to the following information:
  - Name and address;
  - Date and place of birth;
  - Social security number;
  - ABO blood type and Rh factor;
  - Type of injury;
  - Date and time of treatment;
  - Date and time of death, if applicable; and
  - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

### **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

### **PROCEDURES**

1. The Privacy Officer will document any disclosures by whistleblowers and victims of crime, when it is brought to the Privacy Officer's attention that such disclosures have been made.
2. The Privacy Officer will assure that such disclosures have been made to the appropriate parties as described in this Plan's Policy Statement above.
3. The Privacy Officer will retain documentation related to such disclosures in accordance with the Plan's Record Retention policy.
4. Any disclosure for a victim of crime will be limited to the eight items described in the policy section above.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.502(j).
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR POLICIES AND PROCEDURES FOR COMPLIANCE WITH HIPAA PRIVACY REGULATIONS

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(i) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. The Plan will implement policies and procedures with respect to protected health information (PHI). The Policies and procedures will be designed to comply with the standards, implementation specifications, or other requirements of the Privacy regulations.
2. The policies and procedures will be reasonably designed, taking into account the size of and the type of activities of this Plan that relate to protected health information undertaken by the Plan, to ensure such compliance.
3. **Changes to policies or procedures:** The Plan will change its policies and procedures as necessary and appropriate to comply with changes in the law.
  - a. When the Plan changes a privacy practice that is stated in the Plan's HIPAA Privacy Notice and makes corresponding changes to its policies and procedures, the Plan will make the changes effective for protected health information that the Plan creates or receives prior to the effective date of the HIPAA Privacy Notice revision, if the Plan has included in the HIPAA Privacy Notice a statement reserving the Plan's right to make such a change in its privacy practices; or
  - b. The Plan may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with the regulations (as outlined in the section of this policy regarding changes to policies or procedures that do NOT affect the HIPAA Privacy Notice).
4. **Changes in law:** Whenever there is a change in law that necessitates a change to the Plan's policies or procedures, the Plan will promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Plan's HIPAA Privacy Notice the Plan will promptly make the appropriate revisions to the Notice.
5. **Changes to privacy practices that are stated in the HIPAA Privacy Notice:** To implement a change the Plan will:
  - a. Ensure that the policy or procedure, is revised to reflect a change in the Plan's privacy practice as stated in the Plan's Notice;
  - b. Document the policy or procedure, as revised;
  - c. Revise the HIPAA Privacy Notice to state the changed practice and make the revised HIPAA Privacy Notice available as required by the regulations at § 164.520(c). See also this Plan's policy on Privacy Notices for information on the Distribution of the Privacy Notice;
  - d. The Plan will not implement a change to a policy or procedure prior to the effective date of the revised notice; and
  - e. If the Plan has not reserved its right to change a privacy practice as stated in the Plan's HIPAA Privacy Notice, the Plan will be bound by the privacy practices as stated in the Notice with respect to protected health information created or received while such Notice is in effect. The Plan may change a privacy practice that is stated in the Notice, and the related policies and procedures, without having reserved the right to do so, provided that:
    - Such change meets the implementation specifications 164.530(i)(4)(i)(A)-(C) of the regulations; and
    - Such change is effective only with respect to protected health information created or received after the effective date of the Notice.
6. **Changes to policies or procedures that do NOT affect the HIPAA Privacy Notice:** The Plan may change, at any time, a policy or procedure that does not materially affect the content of the Plan's HIPAA Privacy Notice provided that:
  - The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of the regulations; and
  - Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by the regulations.

## **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

## **PROCEDURES**

1. The Privacy Officer will retain documentation of policies and procedures and all changes in policies and procedures in accordance with the Plan's policy on Record Retention.
2. All policies and procedures are to be authorized by the Privacy Officer.
3. Proposed changes to a policy or procedure should be submitted in writing to the Privacy Officer.
4. If a change to a policy/procedure causes a material change to be made to the Plan's HIPAA Privacy Notice, Plan staff will follow the steps to be taken for a material change of a HIPAA Privacy notice. See the Policy/procedure on Privacy Notice in this manual.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.530.
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE ON ACCESS TO PHI

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.524 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Individual's Access to PHI:** The Plan will permit an individual to inspect and obtain a copy of protected health information (PHI) about the individual in a designated record set for as long as the PHI is maintained in the **designated record set**, except for:
  - a. Psychotherapy notes;
  - b. Information compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding; or
  - c. (until October 6, 2014), protected health information maintained by the Plan that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or exempt from the Clinical Laboratory Improvements Amendments of 1988, 42 CFR 493.3(a)(2). Starting October 6, 2014, upon the request of a patient (or the patient's personal representative), the Plan may provide the patient, the patient's personal representative, or a person designated by the patient, as applicable, with copies of completed test reports that it has in its possession that can be identified as belonging to that patient.

The Plan will document the following and retain the documentation:

- The designated record sets that are subject to access by individuals; and
- The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

The Plan may require individuals to make requests for access in writing, provided that the Plan informs individuals of such a requirement. See also item 4 in this Policy for more information on timeliness.

The Plan must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Plan need only produce the PHI once in response to a request for access.

If the Plan does not maintain the PHI that is the subject of the individual's request for access, and the Plan knows where the requested information is maintained, the Plan must inform the individual where to direct the request for access to PHI.

2. **Plan's Denial of an Individual's Access to PHI:**

**The Plan may deny an individual access to PHI without providing the individual the opportunity for review, as follows:**

- a. If the information is excepted from the right of access by paragraph 1 a-c above;
- b. If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
- c. An individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law;
- d. The Plan that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate; or
- e. An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

**The Plan must provide a timely, written denial to the individual, and the denial must be in plain language and contain:**

- The basis for the denial;
- If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights; and
- A description of how the individual may complain to the Plan or to the Secretary of HHS. The description must include the name, or title, and telephone number of the Plan's Privacy Officer.

**3. Individual's Right to Have a Denial of Access to PHI Reviewed:** The Plan may deny an individual access to PHI, provided that the individual is given a right to have such denial reviewed in the following circumstances:

- a. When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- b. When the PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- c. When the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If access is denied on a ground permitted above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Plan to act as a reviewing Officer and who did not participate in the original decision to deny. The Plan must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination. The Plan must provide or deny access in accordance with the determination of the reviewing Officer.

**4. Timely Action by the Plan to a Request to Access PHI.** The Plan will act on a request for access no later than 30 days after receipt of the request as follows.

- a. If the Plan grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested;
- b. If the Plan denies the request, in whole or in part, it must provide the individual with a written denial;
- c. If the request for access is for PHI that is not maintained or accessible to the Plan on-site, the Plan must take an action by no later than 60 days from the receipt of such a request. If the Plan is unable to take an action required within the time required the Plan may extend the time for such action by no more than 30 days, provided that the Plan provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request. The Plan may have only one such extension of time for action on a request for access;
- d. The Plan must arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mail the copy of the PHI at the individual's request. The Plan may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access; or
- e. If an individual's request for access directs the Plan to transmit the copy of protected health information directly to another person designated by the individual, the Plan must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

**5. Plan's Obligation to Provide PHI in Form/Format Requested:** The Plan must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the Plan and the individual.

If the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the Plan must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Plan and the individual.

The Plan may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to such a summary or explanation and the individual agrees in advance to the fees imposed, if any, by the Plan for such summary or explanation.

**6. Fees:** If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the Plan may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

- a. Copying, whether in paper or electronic, including the cost of supplies (for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media such as a CD or flash drive) and labor of copying (including time spent to create and copy the electronic file, such as compiling, extracting, scanning, and burning PHI to electronic media and distribution of the electronic media), the PHI requested by the individual;
- b. Postage, when the individual has requested the copy or electronic media, or the summary or explanation, be mailed; and
- c. Preparing an explanation or summary of the PHI, if agreed to by the individual.
- d. The Plan may not charge retrieval fees (a standard retrieval fee, a fee for the actual cost of retrieval), or fees associated with maintaining systems and recouping capital for data access, storage and infrastructure.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Designated record set** means, at a minimum, the records maintained by or for the Plan relating to the covered individual's enrollment, payment, claims adjudication, case or medical management record systems that are used in whole or in part by the Plan to make decisions about individuals. Records that otherwise meet the definition of designated record set and which are held by a business associate, when acting on behalf of the Plan, are part of the Plan's designated record set.

Designated Record set does not include, psychotherapy notes, claim audit files, records prepared for litigation, health information that is not used to make decisions about individuals or information that the individual does not have a right to access based on state or Federal law, quality and operational improvement records, risk management records. The Privacy Officer (or designee) is responsible for determining what constitutes the designated record set of this Plan.

- **Record** means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Plan. The record may contain electronic and paper documents.

## PROCEDURES

1. A covered individual under the Plan or a personal representative of such individual may request the right to inspect and/or copy PHI pertaining to the covered individual in a "designated record set" (defined above).
2. A request to have access to PHI, to inspect and/or copy PHI must be made (in writing) on a form provided by the Plan and mailed to the Privacy Officer. (See the Request for Access to PHI Form.)
3. If a personal representative makes the request, there must be a proper authorization on file in accordance with the Plan's Personal Representative Policy.
4. **The Privacy Officer or designee will act on a properly filed request within 30 days of receipt of the request** (60 days if the PHI is not maintained onsite), unless an extension is necessary, as outlined in the policy section 4 above.
5. **If the request is approved**, the individual will be notified of the approval and access will be provided.
6. **If the request is denied**, a denial notice will be provided stating the basis for denial (see sample form). The Plan will provide a statement of the right of the individual to have the denial reviewed and a description of how the individual may file a complaint with the Plan and the Secretary of the U.S. Department of Health and Human Services.
7. **Extension:** The time for responding may be extended by 30 days if the Privacy Officer is unable to act upon the request and the individual is notified in writing of the need for extension within 30 days of receipt of the request (See the sample Extension notice).
8. If the Plan does not maintain the PHI that is the subject of the request, and the Plan knows where the requested information is maintained, it will inform the individual where to direct their request for access to PHI.
9. The Plan will assess which of its Business Associates should be made aware of the existence of the request to access PHI and route a copy of the written request to that Business Associate (BA). The Plan will retain proof of such notification to a BA.
10. The Plan will provide the individual with access to the PHI in a timely manner in the hard copy or electronic form and format requested by the individual, if it is readily producible in such form and format. If the PHI is not readily available, the Plan will provide the PHI in a readable hard copy or electronic form or such other form and format as agreed to by the Plan and the individual. In lieu of providing PHI, the Plan may provide a summary of the PHI requested if the individual agrees in advance to the summary and to any fees charged for the summary.
  - If the individual requests PHI in hard copy format, the Plan must provide a readable hard copy format.

- If the individual requests electronic format PHI (ePHI), the Plan must provide a readable electronic format.
  - The Plan is not required to convert hard copy PHI into electronic information to meet an individual's request.
  - With regard to requests for ePHI, the Plan is not required to obtain new types of technology to comply with individual requests.
11. The Plan will arrange with the individual for a convenient time and place to inspect or obtain a copy of the information, or mail a copy of the information at the individual's request.
  12. The Plan will **deny the right to access PHI, to inspect and copy the PHI**, based upon the opinion of a licensed health care professional, that the access requested by the individual or their personal representative, is reasonably likely to cause substantial harm to the individual or another person.
  13. The Plan will deny the right to access PHI , to inspect and copy the PHI if it makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person.
  12. If access is denied for the reasons stated in the Policy Statement, the individual has the right to have the denial promptly reviewed by a licensed health care professional designated as a reviewing officer who did not participate in the original decision. The Plan will designate an unrelated and different licensed health care professional to act as the reviewing officer in such cases.
  13. The Plan reserves the right to charge a fee for copying or postage or requested document preparation. Fees charged are in accordance with the City's Fee Schedule which is available at [www.stocktongov.com](http://www.stocktongov.com), and which addresses the following types of fees:
    - a. Costs of copying or creating PHI for electronic or hardcopy information including labor and supplies,
    - b. Postage for mailing the PHI, and
    - c. The cost of preparing a summary of PHI.

The Plan will not charge retrieval fees (a standard retrieval fee, a fee for the actual cost of retrieval), or fees associated with maintaining systems and recouping capital for data access, storage and infrastructure.
  14. The Plan's Privacy Officer will consult with legal counsel when the request for access to PHI does not appear to fall within the permitted parameters of this Policy and appears to need to be denied in whole or in part.
  15. The Plan will keep all records associated with this policy in accordance with Plan's policy on Record Retention.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.524
- CLIA information: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-06/pdf/2014-02280.pdf>
- The Plan's Privacy Officer

CITY OF STOCKTON

Request for Access to Protected Health Information (PHI)

Today's Date: \_\_\_\_\_, 20\_\_\_\_

Name of Individual for Whom PHI is Requested: \_\_\_\_\_

Name of Individual Requesting Access to PHI: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

I \_\_\_\_\_ am requesting that I be allowed to inspect and copy the following PHI for the above named individual (insert description of PHI being requested including dates):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

*For internal use only:*

The above request for access to PHI has been:

Approved

Plan needs an Extension because:

\_\_\_\_\_

Denied, for the following reason(s):

\_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

CITY OF STOCKTON

Notice of Extension to Decide Request for Access to PHI

Date: \_\_\_\_\_, 20\_\_\_\_\_

To:

[insert name of Individual Requesting Access to PHI]

[insert address of Individual]

Your request for access to protected health information (PHI) was received by the Plan on \_\_\_\_\_; however, a decision on that request will be delayed for [\_\_\_\_ days until \_\_\_\_\_(insert date)] [30 days until \_\_\_\_\_(insert date)]. You will be notified of the decision on your request at or before this date.

The Plan’s decision is being delayed for the following reason(s):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Name of Privacy Officer: \_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_

Once completed, please return this form to the:  
City of Stockton Deputy Director of Human Resources – Risk & Benefits  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

**CITY OF STOCKTON**  
**Notice of Denial of Access to PHI**

---

---

Date: \_\_\_\_\_, 20\_\_\_\_\_

To:

*[insert name of Individual Requesting Access to PHI]*

*[insert address of Individual]*

Your request for access to protected health information (PHI) was received by the Plan on \_\_\_\_\_;  
however, your request is

denied in whole for the following reason:

\_\_\_\_\_.

denied in part. The part that is approved is \_\_\_\_\_. The part that is denied  
is \_\_\_\_\_ and access was denied for this reason

\_\_\_\_\_.

For the portion of your request for PHI that was approved, you will be provided access to that information on  
\_\_\_\_\_ by contacting \_\_\_\_\_ at \_\_\_\_\_.

This denial [is] [is not] subject to appeal. [To appeal, follow these steps: \_\_\_\_\_].

You may file a complaint regarding this Plan's decision to not allow access to all or part of the request for PHI. To  
file a complaint with the Plan's Privacy Officer, please send your written complain to: \_\_\_\_\_.

You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services addressed  
to: The Hubert H. Humphrey Building, 200 Independence Avenue, S. W. Washington D. C. 20201. The complaint  
must be in writing, either in paper or electronic and must name the plan that is the subject of the complaint, describe  
the acts or omission believed to be in violation of the Privacy Standards and must be filed within 180 days after  
receipt of this denial of access to PHI.

---

---

Name of Privacy Officer: \_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_

<p><i>Once completed, please return this form to the:</i> <b>City of Stockton Deputy Director of Human Resources – Risk &amp; Benefits</b> 400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202 Telephone: 209-937-8233 Confidential fax #: 209-937-5702</p>
---

## HIPAA PRIVACY POLICY AND PROCEDURE ON RIGHT TO REQUEST PRIVACY PROTECTION (RESTRICTIONS) ON USE AND DISCLOSURE OF PHI

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.522 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan will permit an individual to request that the Plan **restrict the use and disclosure** of that individual's protected health information (PHI):

- To carry out treatment, payment and health care operations (TPO);
- To persons involved in an individual's care; and
- For notification purposes.

The Plan, however, is **not required to agree to the request to restrict PHI** if the Privacy Officer determines the request to be unreasonable (*for example, if it would interfere with the Plan's ability to pay a claim*).

**EXCEPTION IN EMERGENCY:** If the Plan agrees to the requested restriction, it will not violate the restriction except if the individual is in need of emergency treatment, and the restricted PHI is needed to provide the emergency treatment.

- The Plan may use the restricted PHI, and may disclose this information to a health care provider in order to provide the needed treatment to the individual.
- If restricted PHI is disclosed to a health care provider because it is necessary for emergency treatment, the Plan will request that the health care provider not further use or disclose the information.
- The Plan must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:
  - The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
  - The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

**The Plan's agreement to a restriction on the use or disclosure of PHI is not effective to prevent the following uses or disclosures:**

1. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA, or
2. For instances where an authorization is not required under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.

**The Plan's agreement to a restriction is binding only on the Plan and its business associates, not on other entities such as insurers or health care providers.**

Separately, the Plan acknowledges and understands that **individuals have the right to request that PHI related to services or items for which they have paid out-of-pocket in full, not be disclosed to the Plan**, and that such requests must be granted if the disclosure would be for payment or health care operations purposes and the disclosure is not otherwise required by law. These requests will generally be directed to health care providers, but may result in PHI not being shared with the Plan.

**The Plan will notify its pertinent Business Associates of the existence of a notice of restriction.**

**The Plan must document a restriction and keep the documentation in accordance with record keeping requirements of the Plan.**

**The Plan may terminate the agreement to restrict PHI only if** the following occurs:

1. The individual agrees to or requests the termination in writing;
2. The individual orally agrees to the termination and the oral agreement is documented; or
3. The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

## **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

## **PROCEDURES**

1. A covered individual may request that the Plan restrict any use or disclosure of his/her PHI for:
  - treatment, payment and health care operations;
  - to persons involved in an individual's care;
  - for notification purposes. (See Request for Restriction Form.)
2. An individual must make a written request to the Plan's Privacy Officer to restrict the use or disclosure of PHI:
3. The Privacy Officer will review the written request and notify the covered individual in writing of the Plan's decision to accept or reject the request.
4. The Plan will assess which of its Business Associates should be made aware of the existence of the restriction and route a copy of the notice of restriction to that Business Associate (BA). The Plan will retain proof of such notification to a BA.
5. The Plan's agreement to a restriction on the use or disclosure of PHI is not effective to prevent the following uses or disclosures:
  - a. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA, or
  - b. For instances where an authorization is not required under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.
  - c. The Plan understands that **individuals have the right to request that PHI related to services or items for which they have entirely paid for themselves (out-of-pocket and in full), not be disclosed to the Plan**, and that such requests must be granted if the disclosure would be for payment or health care operations purposes and if the disclosure is not otherwise required by law. These requests will generally be directed to health care providers, but may result in PHI not being shared with the Plan.

*For example, an individual might obtain HIV testing and pay for that lab testing and not submit the claim to a health plan for reimbursement. The provider might have the HIV test results in their files but when our Plan requests health information from the provider, that HIV test result may not be included in the documents sent to us because the patient has requested that the HIV testing they paid for themselves NOT be further shared.*
6. The individual may terminate an agreement to restrict the use and disclosure of PHI by formally revoking his/her request by submitting a signed written request to terminate the agreement (see form).
7. The Plan will assess which of its Business Associates should be made aware of the existence of the revoking of a prior restriction and route a copy of that notice to the Business Associate (BA). The Plan will retain proof of such notification to a BA.
8. Additionally, the Plan may terminate an agreement to restrict the use and disclosure of PHI by notifying the individual in writing. The termination will only be effective for PHI created or received after the date the Plan sends the notice of termination.
9. The Plan will assess which of its Business Associates should be made aware of the existence of the termination of a restriction and route a copy of that notice to the Business Associate (BA). The Plan will retain proof of such notification to a BA.
10. The Privacy Officer will retain documentation of the request for restriction, the Plan's decision and termination of restrictions in accordance with the Plan's Record Retention policy.

**POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

**ADDITIONAL RESOURCES**

- 45 CFR, Section 164.522.
- The Plan's Privacy Officer.

CITY OF STOCKTON

Request For Restrictions On Use And Disclosure Of PHI

Print Name of Individual to Whom the Request Applies: \_\_\_\_\_

Today's Date: \_\_\_\_\_, 20\_\_\_\_\_

I am requesting that use and disclosure of my Protected Health Information (PHI) be **restricted**, in the following manner, effective \_\_\_\_\_ (date):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Signature of Individual Requesting Restriction: \_\_\_\_\_

or

Signature of Personal Representative acting on behalf of the individual, if the individual is not making the Request for Restriction:

\_\_\_\_\_  
\_\_\_\_\_

*Note: The Privacy rules do not contain a requirement to notify individuals of a denial in writing, nor is there a requirement to document requests that are denied. There is also no specific requirement to review denials but this Plan has decided that this paper trail is reasonable and appropriate for their business.*

Your request for restrictions on the use and disclosure of PHI has been:

Approved

Denied, for the following reason(s): \_\_\_\_\_

\_\_\_\_\_

Name of Privacy Officer: \_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_

Date: \_\_\_\_\_

Once completed, please return this form to the:  
City of Stockton Deputy Director of Human Resources – Risk & Benefits  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

CITY OF STOCKTON

Request to Revoke a Prior Restriction on Use & Disclosure of PHI

Print Name of Individual to Whom the Request Applies: \_\_\_\_\_

Today's Date: \_\_\_\_\_, 20\_\_\_\_

Effective \_\_\_\_\_(date), I am revoking a prior request to restrict protected health information and requesting that the Plan no longer honor my prior request to restrict the use and disclosure of Protected Health Information (PHI) that was in effect on \_\_\_\_\_(insert date the request to restrict PHI was implemented).

Signature of Individual Requesting Revocation of the Restriction: \_\_\_\_\_

or

Signature of Personal Representative acting on behalf of the individual: \_\_\_\_\_

Plan staff to attach a copy of the original request to restrict PHI to this revocation form and route to the Privacy Officer for review.

The request to revoke a prior restriction on the use and disclosure of PHI has been:

- Approved and implemented.
Denied, for the following reason(s):\_\_\_\_\_

Name of Privacy Officer: \_\_\_\_\_

Privacy Officer Signature: \_\_\_\_\_ Date: \_\_\_\_\_, 20\_\_\_\_

Once completed, please return this form to the:
City of Stockton Deputy Director of Human Resources - Risk & Benefits
400 E. Main Street, 3rd Floor Stockton CA, 95202
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

## **HIPAA PRIVACY POLICY AND PROCEDURE FOR REQUESTING THAT PHI BE TRANSMITTED CONFIDENTIALLY (e.g. by Alternate Means or Location)**

---

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.522(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

*This policy is drafted without regard to whether there are state medical privacy laws that may be more stringent/restrictive. The Plan will consult legal counsel for interpretation on whether and how state privacy laws impact this group health plan.*

The Plan will permit and accommodate an individual's reasonable request to have PHI sent by alternative means or to an alternative location, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

The Plan will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

### **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

### **PROCEDURES**

1. An individual may request the Plan to transmit PHI by an alternative means or to an alternative location.
2. The request must be in writing (form attached) and mailed or delivered to the Privacy Officer at the following address:

**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

3. The Plan will not require an explanation as to the basis for the request other than having the individual provide a statement that disclosure of the PHI could endanger the individual.
4. The Privacy Officer will review the request to assure the form is completed and request is reasonable and notify the individual if the request is approved or denied.
5. The Plan will only accommodate a reasonable request. For example, a request will be considered reasonable if the request is for mailing to a different address or allowing the individual to personally pick up information that would otherwise be mailed. The alternative address or request to allow a personal pick up must be specified in the request.
6. The Plan will assess which of its Business Associates should be made aware of the existence of the request to transmit PHI by an alternative means or to an alternative location and route a copy of the written request to that Business Associate (BA). The Plan will retain proof of such notification to a BA.
7. The Privacy Officer will retain documentation of the request and the Plan's approval/denial in accordance with the Plan's policy on Record Retention.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.522(b).
- The Plan's Privacy Officer.

CITY OF STOCKTON

Request That PHI Be Transmitted Confidentially

Today's Date: \_\_\_\_\_, 20\_\_\_\_

Print name of individual making request: \_\_\_\_\_

I am requesting that effective (insert date) \_\_\_\_\_, the following protected health information (PHI) (specify PHI) \_\_\_\_\_

be transmitted to me by the alternate means or location described below:

(Insert the new mailing address/place or manner in which individual will receive future information that would otherwise have been mailed to the individual's address the Plan has on file (e.g. will personally pick up.)

I am requesting this confidentiality of PHI because the Plan's current method of disclosure of PHI, to which my request pertains, may endanger me.

Signature of individual requesting confidential transmission of PHI: \_\_\_\_\_

or

Signature of Personal Representative (acting on behalf of the individual) requesting confidential transmission of PHI: \_\_\_\_\_

Your request for confidential communication of PHI has been:

- Approved
Denied, for the following reason(s): \_\_\_\_\_

Name of Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_

Once completed, please return this form to the:
City of Stockton Deputy Director of Human Resources - Risk & Benefits
400 E. Main Street, 3rd Floor Stockton CA, 95202
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

CITY OF STOCKTON

Request to Terminate the Confidential Transmission of PHI

(By Alternate Means/Location)

Today's Date: \_\_\_\_\_, 20\_\_\_\_\_

Print name of individual making request: \_\_\_\_\_

I am requesting that effective (insert date)\_\_\_\_\_, my original request to maintain confidentiality of PHI delivery (e.g. by an alternate means/location) be terminated. Please deliver all future PHI to me at my usual address/location as follows:

(Insert the mailing address or manner or usual place where individual will personally pick up the information.)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Signature of individual requesting termination of confidential transmission of PHI:

\_\_\_\_\_

or

Signature of Personal Representative (acting on behalf of the individual) requesting termination of confidentiality of PHI:

\_\_\_\_\_

The above noted request to terminate confidentiality of PHI has been reviewed and:

- Will be adopted as requested on the date requested above.
- Will be adopted but with these modifications: \_\_\_\_\_
- Cannot be adopted because (insert reason(s)): \_\_\_\_\_

Name of Privacy Officer: \_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_, 20\_\_\_\_\_

Once completed, please return this form to the:  
City of Stockton Deputy Director of Human Resources – Risk & Benefits  
400 E. Main Street, 3rd Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

## HIPAA PRIVACY POLICY AND PROCEDURE ON RIGHT TO AMEND PHI

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.526 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Right to amend:** An individual has the right to have the Plan amend protected health information (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.
2. **Denial of amendment:** The Plan may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:
  - a. Was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
  - b. Is not part of the designated record set;
  - c. Would not be available for inspection under the "Access to PHI" policy; or
  - d. Is accurate and complete.
3. **Individual's request for amendment:** The Plan must permit an individual to request that the Plan amend the PHI maintained in the designated record set. The Plan may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. The right to amend PHI applies only for as long as the PHI is maintained in a designated record set.
4. **Timely action by the Plan:** The Plan must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.
  - a. If the Plan grants the requested amendment, in whole or in part, it must take the actions required by paragraphs 5a and b below.
  - b. If the Plan denies the requested amendment, in whole or in part, it must provide the individual with a timely written denial as outlined in this policy.

If the Plan is unable to act on the amendment within the time required by this policy, the Plan may extend the time for such action by no more than 30 days, provided that:

  - a. The Plan, no later than 60 days after receipt of such a request, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request; and
  - b. The Plan may have **only one such extension** of time for action on a request for an amendment.
5. **Accepting the amendment:** If the Plan accepts the requested amendment, in whole or in part, the Plan must comply with the following requirements.
  - a. **Making the Amendment:** The Plan must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. The right to amend does not include the right for a covered individual to make the actual changes to PHI.
  - b. **Informing the Individual:** The Plan must timely inform the individual that the amendment is accepted and obtain the individual's identification of, and agreement to have the Plan notify the relevant persons with which the amendment needs to be shared in accordance with the following paragraph 5c.
  - c. **Informing Others:** The Plan must make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - Persons identified by the individual as having received protected health information about the individual and needing the amendment; and
    - Persons, including business associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

6. **Denying the amendment:** If the Plan denies the requested amendment, in whole or in part, the Plan must comply with the following requirements.
- a. Provide the individual with a timely, written denial, in accordance with this policy. The **denial must use plain language and contain:**
    - The basis for the denial (see paragraph 2 above);
    - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
    - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
    - A description of how the individual may complain to the Plan or to the HHS Secretary. The description must include the name, or title, and telephone number of the Privacy Officer.
7. **Statement of disagreement:** The Plan must permit the individual to submit to the Plan a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Plan may reasonably limit the length of a statement of disagreement. The Plan may prepare a written **rebuttal** to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the Plan must provide a copy to the individual who submitted the statement of disagreement.
8. **Recordkeeping:** The Plan must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any, to the designated record set.
9. **Future disclosures:** If a statement of disagreement has been submitted by the individual, the Plan must include the material appended in accordance with paragraph 7 above, or, at the election of the Plan, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
- If the individual has not submitted a written statement of disagreement, the Plan must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action in accordance with paragraph 6a above.
- When a subsequent disclosure is made using a standard HIPAA Electronic Data Interchange (EDI) transaction that does not permit the additional material to be included with the disclosure, the Plan may separately transmit the material, as applicable, to the recipient of the standard transaction.
10. **Actions on notices of amendment:** If the Plan is informed by another covered entity (group health plan, health care provider or clearinghouse) of an amendment to an individual's PHI, in accordance with paragraph 5c above, the Plan must amend the PHI in designated record sets as provided by paragraph 5a above.
11. **Documentation:** The Plan must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by the regulations (see this Plan's policy on Record Retention).

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Designated record set means**, at a minimum, the records maintained by or for the Plan relating to the covered individual's enrollment, payment, claims adjudication, case or medical management record systems that are used in whole or in part by the Plan to make decisions about individuals. Records that otherwise meet the definition of designated record set and which are held by a business associate, when acting on behalf of the Plan, are part of the Plan's designated record set.

Designated Record set does not include, psychotherapy notes, claim audit files, records prepared for litigation, health information that is not used to make decisions about individuals or information that the individual does not have a right to access based on state or Federal law, quality and operational improvement records, risk management records. The Privacy Officer (or designee) is responsible for determining what constitutes the designated record set of this Plan.

- **Record means** any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Plan. The record may contain electronic and paper documents.

## PROCEDURES

1. A covered individual may request the Plan to amend PHI pertaining to that individual. The PHI must be in a designated record set maintained by the Plan.
2. A request must be in writing, provide a reason for the request and be mailed to the Privacy Officer at their address listed on the Cover Page of this manual. See also the form titled "Request to Amend PHI."
3. **Timing of Decision:** The Plan will act on the request within 60 days of receipt of the request. The Plan may extend the time to comply by 30 days, provided that the Plan notifies the individual in writing within the first 60 days and explains the reasons for the delay and the date by which the Plan will act.
4. **Reason for Denial:** The Plan will deny the request for amendment if the Privacy Officer determines that the PHI or other record:
  - a. Was not created by the Plan, unless the individual provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the request;
  - b. Is not part of the designated record set;
  - c. Is not available for inspection under HIPAA (in accordance with the Plan's Policy for Access to PHI); or
  - d. Is accurate and complete.
5. **Accepting the Amendment:** If the Plan accepts the request for the amendment in whole or in part, then the Plan will do the following:
  - a. Make the appropriate amendment to PHI by providing a link to the affected records or append the affected records within 60 days of the receipt of the request.

*Note: The privacy rules do not require that Plans delete or expunge any PHI from their records. The Plan can simply provide a link within the affected document to the amendment. Also, individuals requesting an amendment have no right under the privacy rule to determine the content of any amendment that is made. Individuals do not have the right to make the actual changes to their PHI. It is within the Plan's discretion to make the appropriate amendment.*
  - b. Within 60 days of the receipt of the request, inform the individual of the amendment that will be made and obtain from the individual the identification of and an agreement to have the Plan notify persons who should be aware of the amendment.
  - c. Make reasonable efforts to provide the amendment to persons identified by the individual or persons, including business associates that the Plan knows may have or could rely on the PHI to the detriment of the individual.
6. **Denying the Amendment:** If the request to amend is denied, in whole or in part, then the Privacy Officer (or designee) will provide a denial notice containing the following information:
  - a. Basis for denial;
  - b. A statement of the individual's right to submit a statement of disagreement with the denial, and how this statement can be filed;
  - c. A statement that if an individual does not submit a statement of disagreement, the individual has a right to request that the Plan furnish a copy of the Request for amendment and Denial of the request with future disclosures of the PHI that was the subject of the request; and
  - d. A description of how an individual can file a complaint with the Plan and the Secretary of the U.S. Department of Health and Human services.
7. **Statement of Disagreement:** Where the request to amend is denied, the individual may submit a written statement disagreeing with the denial and explaining the basis for the disagreement.
8. **Rebuttal Statement:** The Plan through its Privacy Officer may then issue a written rebuttal to the individual's statement of disagreement. If the Plan prepares a rebuttal statement, a copy of the rebuttal will be provided to the individual who submitted the statement of disagreement.
9. **Recordkeeping:** The request for amendment, the denial, any statement of disagreement and any rebuttal statement will be linked or appended to the related PHI kept in the designated record set. Documents will be retained in accordance with the Plan's policy on Record Retention.

**10. Future Disclosures:**

- a. If a statement of disagreement has been submitted, the statement or a summary of the statement will be attached to any subsequent disclosure of the PHI.
  - b. If a statement of disagreement has not been submitted, then the Plan will (upon the individual's request) include the individual's request for amendment and the denial (or a summary of this information) with any subsequent disclosure of the PHI.
  - c. When a subsequent disclosure is made in the form of an electronic transmission that is a standard transaction under HIPAA's Electronic Data Interchange ("EDI") rules, the required information will be sent separately to the recipient of the information, if the transaction does not permit the additional material to be included with the disclosure.
11. **Action Amendment Made By Other Covered Entities:** Upon notification of an amendment to PHI by another covered entity (e.g. another health plan or medical provider), the Plan will amend the PHI in its designated record set.
12. The Plan will assess which of its Business Associates should be made aware of the existence of the request to amend PHI and route a copy of the written request to that Business Associate (BA). The Plan will retain proof of such notification to a BA.

**POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

**ADDITIONAL RESOURCES**

- 45 CFR, Section 164.526
- The Plan's Privacy Officer

CITY OF STOCKTON

Request to Amend Protected Health Information (PHI)

Today's Date: \_\_\_\_\_, 20\_\_\_\_

Name of Individual for whom PHI amendment is requested: \_\_\_\_\_

Name of Individual Requesting Amendment of PHI: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

I \_\_\_\_\_ am requesting that an amendment be made to the following PHI

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

for the following reason(s):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

If this request is approved, I hereby request that the following individuals, business associates or other covered entities be notified:

\_\_\_\_\_  
\_\_\_\_\_

*For internal use only:*

The above request for amendment to the above noted PHI has been:

Approved

Denied, for the following reason(s):

\_\_\_\_\_  
\_\_\_\_\_

Signature of Privacy Officer: \_\_\_\_\_ Date: \_\_\_\_\_

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
Telephone: 209-937-8233 Confidential fax #: 209-937-5702

## HIPAA PRIVACY POLICY AND PROCEDURE ON THE RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to section 164.528 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Individual Rights:** An individual has a **right to receive an accounting of disclosures of protected health information (PHI) made by the Plan in the six years prior** to the date on which the accounting is requested, **except for** disclosures:
  - a. To carry out treatment, payment and health care operations;
  - b. To individuals referencing the PHI about themselves;
  - c. Incident to a use or disclosure otherwise permitted or required by the privacy regulation;
  - d. Pursuant to an authorization;
  - e. For the facility's directory or to persons involved in the individual's care or other notification purposes (§ 164.510);
  - f. For national security or intelligence purposes as provided in section 164.512(k)(2);
  - g. To correctional institutions or law enforcement officials as provided in section 164.512(k)(5);
  - h. As part of a limited data set in accordance with section 164.514(e); or
  - i. That occurred prior to the compliance date for the Plan.
2. **Suspension of Rights:** The Plan must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, (as provided in § 164.512(d) or (f), respectively), for the time specified by such agency or official, if such agency or official provides the Plan with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made **orally**, the Plan must:
  - a. Document the statement, including the identity of the agency or official making the statement;
  - b. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
  - c. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

An individual may request an accounting of disclosures for a period of time **less than** six years from the date of the request.

3. **Content of the accounting.** The Plan must provide the individual with a written accounting that meets the following requirements.
  - a. The accounting must include disclosures of PHI that occurred during the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of the Plan.
  - b. The **accounting must include** for each disclosure:
    - The date of the disclosure;
    - The name of the entity or person who received the PHI and, if known, the address of such entity or person;
    - A brief description of the PHI disclosed; and
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of a written request for a disclosure, if any, (see also sections 164.502(a)(2)(ii) or 164.512,).

If, during the period covered by the accounting, the Plan has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

- The information required for the first disclosure during the accounting period;
  - The frequency, periodicity, or number of the disclosures made during the accounting period; and
  - The date of the last such disclosure during the accounting period.
- If, during the period covered by the accounting, the Plan has made disclosures of PHI for a particular research purpose for 50 or more individuals (in accordance with §164.512(i)), the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

- a.) The name of the protocol or other research activity;
- b.) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
- c.) A brief description of the type of PHI that was disclosed;
- d.) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
- e.) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
- f.) A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If the Plan provides an accounting for research disclosures, (in accordance with 164.528(b)(4)), and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Plan will, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

4. **Provision of the accounting:** The Plan must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:
  - a. The Plan must provide the individual with the accounting requested; or
  - b. If the Plan is unable to provide the accounting within the time required, the Plan may extend the time to provide the accounting by no more than 30 days, provided that:
    - The Plan, within 60 days after receipt of such a request, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will provide the accounting; and
    - The Plan may have only one such extension of time for action on a request for an accounting.
  - c. The Plan will provide the first accounting to an individual in any 12-month period without charge.
  - d. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the Plan informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
5. **Documentation:** The Plan must document the following and retain the documentation for six years:
  - a. The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;
  - b. The written accounting that is provided to the individual under this section; and
  - c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

## KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Reasonable, cost-based fee** means postage, supplies, labor related to copying. It does not mean cost/labor associated with searching for and retrieving the requested information.

## PROCEDURES

*It is important to note that only "disclosures" and not "uses" currently have to be included in an accounting. Many disclosures are not subject to the accounting requirements such as disclosures for TPO, disclosures to an individual that were about that individual, incidental disclosures, and disclosures pursuant to an authorization form.*

1. An individual who requests an accounting must use the form entitled Request for Accounting of Disclosures of PHI.
2. The Privacy Officer will provide a form titled "Request for Accounting of Disclosures of PHI" to any individual who wishes to request an accounting of disclosures.
3. The form must be completed and signed by the individual. The individual may mail, fax or deliver the form to the Privacy Officer at their address listed on the Cover Page of this Manual.
4. The Privacy Officer or designee will review the form and prepare a written Accounting of all uses and disclosures for which Accounting is required. In general, an Accounting is required for the disclosure of (PHI) if the disclosure occurs outside the scope of treatment, payment and health care operations, and is not made as a result of a signed authorization. An Accounting is required for all of the following Uses and Disclosures of PHI:
  - a. As required by law (§512 (a));
  - b. For public health activities (§512 (b));
  - c. About victims of abuse, neglect or domestic violence (§512 (c));

- d. For health oversight activities (§512 (d));
  - e. For judicial and administrative proceedings (§512 (e));
  - f. For law enforcement purposes (§512 (f))
  - g. About decedents (§512 (g));
  - h. For cadaveric organ, eye or tissue donation purposes (§512 (h));
  - i. For research purposes (§512 (i));
  - j. To avert a serious threat to health or safety (§512 (j));
  - k. For specialized government functions (§512 (k)) other than for national security and intelligence activities (§512 (k)(2)) or for correctional institutions and other law enforcement custodial situations (§512 (k) (5));
  - l. For worker's compensation (§512 (l));
  - m. To Secretary of HHS as part of a compliance review (§502 (a) (2) (ii));
  - n. For unlawful or unauthorized (accidental/erroneous) disclosures (§528 (a)(1) and OCR FAQ 204). While 'incidental' disclosures do not have to be included in an accounting, those disclosures that occur in violation of the HIPAA regulation (e.g. accidental/erroneous) are not exempted and should be listed (for example, medical records stolen, e-mailed to wrong person or accessed by unauthorized personnel.)
5. The Privacy Officer will respond as follows:
- a. An Accounting will be provided within 60 days of receipt of the Request for Accounting Form by the Privacy Officer.
  - b. If the Plan is unable to provide the Accounting within 60 days, the Plan will invoke one thirty-day extension, provided the individual is notified by the Privacy Officer in writing within the first 60 days, of the reason for the delay and the date by which the Plan will provide the accounting.
  - c. One Accounting for an individual in a twelve-month period will be provided without charge. The Plan will impose a fee based only on the cost of copying (including labor, supplies and postage) for each additional request during the twelve-month period. However, the Privacy Officer will notify the individual of the fee in advance and allow the individual to modify or withdraw the request.
6. The Plan must temporarily suspend the individual's right to receive an Accounting of such uses and disclosures to a health oversight agency ("agency") or law enforcement official ("official") if a temporary suspension is requested by the agency or official in accordance with the following procedures:
- a. The agency or official states in writing to the Plan that providing such Accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for which the suspension of the right to an Accounting of these disclosures is required, or
  - b. The agency or official orally states to the Plan that providing such Accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for the suspension. The Plan must document the statement (including the identity of the agency or official making the statement) and must limit the temporary suspension to no longer than 30 days from the date of the oral statement (unless a written statement complying with the requirements of paragraph (b) is submitted).
7. With the exception of uses and disclosures of PHI that are **not** subject to an Accounting in accordance with the Plan's Right to Accounting Policy, the Plan must include in an Accounting any uses and disclosures of PHI made during the six years before the date of the Accounting (or fewer years if the Plan's HIPAA compliance date is fewer than six years before the Accounting).
8. Disclosures made to or by Business Associates of the Plan must be included in the Accounting unless it falls into one of the exceptions for the right to an accounting. This means that the Plan must contact each Business Associate and request that the Business Associate provide the Plan with an accounting of disclosures, within the timeframe noted in Step 5 above, so that the Plan can properly notify the requester of the disclosures made by the Plan and its Business Associates.

9. **For each disclosure**, the Accounting must include:
  - a. The date of the disclosure;
  - b. The name of the entity or person who received the PHI and, if known, the address of the entity or person;
  - c. A brief description of the PHI disclosed; and
  - d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure, if any.
10. To the extent that the Plan has made **multiple disclosures of PHI to the same person or entity for a single purpose**, the accounting regarding this multiple disclosure may provide:
  - a. All information that would be otherwise required for the first disclosure in the Accounting period;
  - b. The frequency, periodicity or number of disclosures made during the Accounting period; and
  - c. The date of the last such disclosure in the Accounting period.
11. To the extent that the Plan has made **disclosures for research purposes** (under section 164.512(i) of the privacy rules) for 50 or more individuals, the Accounting may provide:
  - a. The name of the protocol or research activity;
  - b. A plain language description of the protocol or research activity (including the purpose of the research and the criteria for selecting particular records);
  - c. The type of PHI disclosed;
  - d. The date or period during which the disclosures occurred;
  - e. The name, address and phone number of:
    - i) The entity that sponsored the research; and
    - ii) The researcher to whom the PHI was disclosed; and
  - f. A statement that PHI may or may not have been disclosed for a particular protocol or research purpose.
12. If the Plan provides an **accounting for research purposes**, and if it is reasonably likely that this PHI was disclosed for such research, protocol, or activity, the Plan will, upon the individual's request, assist in contacting the entity that sponsored the research and the researcher.
13. The Plan reserves the right to charge a reasonable fee.
 

The Plan may charge a fee for copying or postage or requested document preparation. Fees charged are in accordance with the City's Fee Schedule which is available at [www.stocktongov.com](http://www.stocktongov.com), and which addresses the following types of fees:

  - a. Costs of copying or creating PHI for electronic or hardcopy information including labor and supplies,
  - b. Postage for mailing the PHI, and
  - c. The cost of preparing a summary of PHI.
14. **Documentation:** The Plan will keep any information that is the subject of an accounting and any written accounting according to its Record Retention policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR 164.528
- The Plan's Privacy Officer



## HIPAA PRIVACY POLICY AND PROCEDURE FOR WAIVER OF RIGHTS

---

### **POLICY STATEMENT**

This policy and procedure is adopted pursuant to Section 164.530(h) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan **may not** require individuals to waive their rights to file a complaint with the Secretary (section 164.306) or any other rights guaranteed under the HIPAA Privacy regulations as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

### **KEY DEFINITIONS**

For assistance understanding common terms used in this manual, refer to the cover page.

### **PROCEDURES**

1. The Privacy Officer will assure that enrollment forms, forms used to administer these Privacy rules and other information related to the Plan contain no wording that could be construed to require that individuals waive any rights guaranteed under the HIPAA Privacy regulations.
2. The Privacy Officer will document those forms that have been reviewed and approved for compliance with this rule.

### **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

### **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.530(h).
- The Plan's Privacy Officer.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR LIMITED DATA SET

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514(e) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

- 1. Limited data set:** The Plan may use or disclose a limited data set of PHI that meets the definition of limited data set along with the requirements of paragraph 2 below, if the Plan enters into a data use agreement with the limited data set recipient, in accordance with paragraph 3 of this policy.
- 2. Permitted purposes for uses and disclosures:** The Plan may use or disclose a limited data set (as defined in these policies and procedures) only for the purposes of research, public health, or health care operations. The Plan may use PHI to create a limited data set that meets the definition of limited data set, or disclose PHI only to a business associate for such purpose, whether or not the limited data set is to be used by the Plan.
- 3. Data Use Agreement:** The Plan may use or disclose a limited data set under paragraph 1 of this policy only if the Plan obtains satisfactory assurance, in the form of a “data use agreement” that meets the requirements of this policy, that the limited data set recipient will only use or disclose the PHI for limited purposes.

**Contents of a Data Use Agreement.** A data use agreement between the Plan and the limited data set recipient must:

- Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph 2 of this policy. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the Plan.
- Establish who is permitted to use or receive the limited data set and provide that the limited data set recipient will:
  - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  - Use appropriate safeguards to prevent use or disclosure of the information, including electronic protected health information, other than as provided for by the data use agreement;
  - Report to the Plan any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
  - Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
  - Not identify the information or contact the individuals

*(Because it is not anticipated that the Plan will use a Data Use Agreement very often, no draft Data Use Agreement form has yet been created.)*

- 4. Compliance:** The Plan is not in compliance with the standards of this policy if the Plan knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the Plan took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
  - Discontinued disclosure of protected health information to the recipient; and
  - Reported the problem to the Secretary of HHS.

If this Plan is a limited data set recipient and violates a data use agreement this Plan will be in noncompliance with the standards, implementation specifications, and requirements of this policy.

### KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

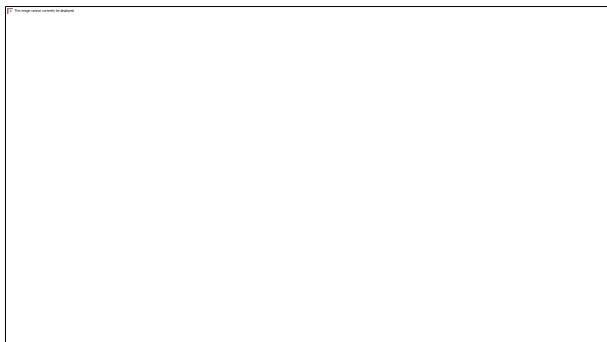
- Limited data set means** protected health information that **excludes** the following direct identifiers of the individual or of relatives, employers, or household members of the individual
  - Names;
  - Postal address information, other than town or city, State, and zip code;
  - Telephone numbers and fax numbers;
  - Electronic mail addresses;

- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

The following direct identifiers **are not part of a limited data set**:

- admission;
- discharge and service dates;
- date of death;
- age; and
- five digit zip code (*\*for public health, research or health care operations*).

\*See: <http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm> (Box 3) or [https://privacyruleandresearch.nih.gov/pr\\_08.asp](https://privacyruleandresearch.nih.gov/pr_08.asp)



## **PROCEDURES**

1. The Privacy Officer will be responsible for assuring that release of PHI under these limited data set policies is properly administered.
2. The Privacy Officer will work with legal counsel if a data use agreement document needs to be created.
3. In assuring that release of PHI under these limited data set policies, the Privacy Officer will keep in mind those items that are not considered to be part of the limited data set (as defined above) and are therefore permitted, to be released without using a limited data set.
4. The Privacy Officer will retain documentation related to the use of limited data sets in accordance with the Plan's Record Retention policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Section 164.514(e).
- The Plan's Privacy Officer.

# HIPAA PRIVACY POLICY AND PROCEDURE FOR FUNDRAISING AND UNDERWRITING

---

## POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514(f) and (g) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. **Uses and disclosures of PHI for Fundraising.** The Plan may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without a valid authorization:
  - a. Demographic information relating to an individual, including name, address, other contact information, age, gender and date of birth;
  - b. Dates of health care provided to an individual;
  - c. Department or service information;
  - d. Treating physician;
  - e. Outcome information and;
  - f. Health insurance status.

The Plan may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph 1 of this policy unless a statement is included in the Plan's HIPAA Privacy Notice (as required by § 164.520(b)(1)(iii)(B)).

The Plan must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

- The Plan may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.
- The Plan may not make fundraising communications to an individual where the individual has elected not to receive such communications.
- The Plan may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

2. **Uses and disclosures of PHI for Underwriting and related purposes:**

If a health plan receives protected health information for the purpose of underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose as may be required by law, subject to the prohibition with respect to genetic information included in the protected health information. See also the policy/procedure in this manual related to Limitations on the Use and Disclosure of Genetic Information.

This Plan will remind all health plans that receive PHI for underwriting of the above requirements.

## KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

## PROCEDURES

1. This Plan will not use PHI to perform fundraising activities.
2. When the Plan initiates a competitive bid for health benefits that are subject to the HIPAA Privacy regulations, the Privacy Officer will request that such bid include a statement about the underwriting requirements of this Plan (according to paragraph 2 in the policy above), and that the recipient of a competitive bid from this Plan may not use or disclose PHI that was provided to that health plan for underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits for any other purpose, except as may be required by law.
3. The Privacy Officer will retain documentation in accordance with the Plan's Record Retention policy.

**POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions and Limitations on the Use and Disclosure of Genetic Information.

**ADDITIONAL RESOURCES**

- 45 CFR, Section 164. 514(f) and (g).
- The Plan's Privacy Officer.
- Refer to the policy on Authorizations.

## HIPAA PRIVACY POLICY AND PROCEDURE FOR MARKETING AND PROHIBITION ON SALE OF PHI

---

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.501, 164.508(a)(3) and (a)(4), and 164.502(a)(5)(ii) of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

#### Marketing

Section 164.508 (a) addresses that an **authorization is required for marketing**. The authorization must state the Plan will receive financial remuneration from or on behalf of the third party whose items or services are being marketed, and must be signed and received by the Plan before the marketing activity begins.

Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing.

If the marketing involves direct or indirect financial remuneration (defined in this policy under Key Definitions) to the covered entity from a third party, the authorization must state such remuneration is involved.

#### Prohibition on Sale of PHI Policy

Subject to the exceptions below, the Plan will obtain an authorization to disclose PHI if it is receiving direct or indirect remuneration from or on behalf of the recipient of the information in exchange for the information. (The authorization must state the Plan will receive remuneration in the form of payment or other benefit for disclosing or selling the PHI, and must be signed and received by the Plan before the marketing activity begins.)

For this purpose, “sale of PHI” includes transactions that involve a transfer of ownership of PHI, as well as exchanges of PHI under access, license or lease agreements, and any other exchanges of PHI for which remuneration is made.

- **Remuneration includes** financial payments or non-financial benefits (such as benefits in-kind).
- **Direct remuneration** is that which is received directly from the recipient of the PHI and **indirect remuneration** is that which is received on behalf of the recipient of the PHI from another entity.

The following disclosures are an exception from the prohibition on the sale of PHI and therefore, **no authorization is required to make these disclosures** under 164.512(b) or 164.514(e):

- Disclosures for public health purposes under 164.512(b) or 164.514(e);
- For research purposes pursuant to 164.512(i) or 164.514(e) as long as remuneration is subject to certain limitations;
- For treatment and payment purposes;
- For the sale transfer, merger or consolidation of all or part of the Plan and for related due diligence;
- To a business associate for activities that the business associate undertakes on behalf of the Plan, and the only remuneration is for the performance of the business associate activities on behalf of the Plan;
- To an individual who makes a request for access (See the Policy on Right of Access to PHI) or a request for an account of disclosure (see the Policy on Right of Accounting of Disclosures of PHI);
- As required by law as permitted under 164.512(a); and
- For any other purpose permitted by these policies and procedures and the privacy rule, as long as any remuneration is limited to a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for that purpose, or a fee that is permissible by other law.

## KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

As defined in Section 164.501, **marketing means (and an authorization will be obtained):**

- (1) To make a communication (from the Plan or its Business Associate) about a product or service that encourages recipients of the communication to purchase or use the product or service, and for which, in exchange for making the communication, the Plan (or its business associate) receives direct or indirect financial remuneration from the entity whose product or service is being marketed.
  - (i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
  - (ii) For treatment of the individual; or
  - (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
- (2) For marketing purposes, **financial remuneration means** direct payment from the third party whose product or service is being described in the marketing communication, or indirect payment from another entity on behalf of the third party whose product or service is being described in the marketing communication. **Financial remuneration does not include** non-financial benefits such as in-kind benefits, or financial payments made for purposes other than marketing.

Direct or indirect payment does not include any payment for treatment of an individual.

- (3) The following activities are not marketing and therefore can be done without the Plan obtaining an individual's authorization. **Marketing does not include** a communication made:
  - i. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. In addition to refill reminders, these communications may include information about generic equivalents, medication adherence or how to take biologic or self-administered medication. **If the financial remuneration received by the Plan is in excess of the costs reasonably related to making the communication, the communication will be a marketing communication for which authorization is required.**
  - ii. For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:
    - A. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
    - B. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
    - C. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

The following communications are not marketing communications for which an authorization is required even if financial remuneration is received:

- A face to face communications by the entity (the Plan) with the individual whose PHI is being disclosed;
- A promotional gift of nominal value to the individual whose PHI is being disclosed; or
- Communications promoting a healthy diet or encouraging individuals to get certain routine diagnostic tests do not constitute marketing and do not require an authorization.

## PROCEDURES

1. The Plan and Privacy Officer will review a situation/request to determine if this procedure on marketing applies.

Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. The Privacy Rule carves out the following health-related activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;
- Communications for treatment of the individual; and
- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect financial remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services.

2. As a covered entity, the Plan will obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between the Plan and an individual, and for the Plan's provision of promotional gifts of nominal value.

No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition.

An authorization for marketing that involves the Plan's receipt of direct or indirect financial remuneration from a third party must reveal that fact.

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, **the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing.** So as not to interfere with core health care functions, the Rule distinguishes marketing communications from those communications about goods and services that are essential for quality health care. The Privacy Rule addresses the use and disclosure of protected health information for marketing purposes by:

- Defining what is "marketing" under the Rule;
- Excepting from that definition certain treatment or health care operations activities; and
- Requiring individual authorization for all uses or disclosures of protected health information for marketing purposes with limited exceptions.

3. The Privacy Officer will understand that the Privacy Rule defines "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." **Generally, if the communication is "marketing," then the communication can occur only if the covered entity (the Plan) first obtains an individual's "authorization."** This definition of marketing has certain exceptions, as discussed below. Examples of "marketing" communications requiring prior authorization are:

- A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for \$39, when the communication is not for the purpose of providing treatment advice.
- A communication from a health insurer promoting a home and casualty insurance product offered by the same company.

Marketing also means: "An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect financial remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service." This part of the definition to marketing has no exceptions. **The Plan must obtain authorizations before these marketing communications can occur.**

The Plan may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list. For example, it is "marketing" when:

- A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors.
  - A drug manufacturer receives a list of patients from a covered health care provider and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patients.
4. The Privacy Officer will understand that the Privacy Rule carves out exceptions to the definition of marketing under the following three categories:
- (a) A communication is not "marketing" if it is made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:
- The entities participating in a health care provider network or health plan network;
  - Replacement of, or enhancements to, a health plan; and
  - Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
- This exception to the marketing definition permits communications by a covered entity about its own products or services. For example, under this exception, it is not "marketing" when:
- A hospital uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or magnetic resonance image machine) through a general mailing or publication.
  - A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.
- (b) A communication is not "marketing" if it is made for treatment of the individual. For example, under this exception, it is not "marketing" when:
- A pharmacy or other health care provider mails prescription refill reminders to patients, or contracts with a mail house to do so.
  - A primary care physician refers an individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.
- (c) A communication is not "marketing" if it is made for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. For example, under this exception, it is not "marketing" when:
- An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.
  - A hospital social worker shares medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home.

For any of the three exceptions to the definition of marketing, the activity must otherwise be permissible under the Privacy Rule, and the Plan may use a business associate to make the communication. As with any disclosure to a business associate, the Plan must obtain the business associate's agreement to use the protected health information only for the communication activities of the Plan as covered entity.

5. Except as discussed below, any communication that meets the definition of marketing is not permitted, unless the Plan, as covered entity, obtains an individual's authorization. To determine what constitutes an acceptable "authorization," see the Policy/procedure on Authorizations.
- An example of marketing that may need an authorization is for the Plan to give the names and addresses of plan participants to a company that will mail marketing material to them about a Medicare Health Exchange.
6. If the marketing involves direct or indirect financial remuneration to the Plan from a third party, the authorization must state that such remuneration is involved. However, a communication does not require an authorization, even if it is marketing, if it is in the form of a face-to-face communication made by the Plan to an individual; or a promotional gift of nominal value provided by the Plan. For example, no prior authorization is necessary when:
- A hospital provides a free package of formula and other baby products to new mothers as they leave the maternity ward.

- An insurance agent sells a health insurance policy in person to a customer and proceeds to also market a casualty and life insurance policy as well.
7. These procedures are meant to be helpful to the Privacy Officer in determining when an authorization is needed before the Plan can undertake “marketing.” The Privacy Officer will consult with legal counsel as appropriate.
  8. The Plan generally will require an authorization form for the sale of protected health information if the Plan receives direct or indirect financial remuneration (payment) from the entity to which the PHI is sold.

**POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

**ADDITIONAL RESOURCES**

- 45 CFR, Section 164. 501 and 164.508(a).
- The Plan’s Privacy Officer.
- Refer to the policy on Authorizations.

## HIPAA PRIVACY POLICY AND PROCEDURE REGARDING STATE LAWS

---

### POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 160.203-205 of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

This Plan recognizes that certain state laws may be more stringent than the Federal HIPAA Privacy regulation requirements. The Plan will adhere to state laws that are more stringent than the Federal law, where applicable to the Plan.

#### **Preemption of State Law - General Rule and Exception - § 160.203**

A standard, requirement, or implementation specification adopted under the HIPAA Privacy regulations that is **contrary** to a provision of State law preempts the provision of State law. When used to compare a provision of State law to a HIPAA Privacy standard, requirement or implementation specification, **contrary means** that the Plan would find it impossible to comply with both the State and Federal requirements or the state law stands as an obstacle to accomplishing the full purpose and objectives of the Federal law.

This general rule applies, except if one or more of the following conditions is met:

- a. A determination is made by the Secretary of the Department of Health and Human Services (HHS) that the provision of State law is necessary:
  - To prevent fraud and abuse related to the provision of or payment for health care;
  - To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
  - For State reporting on health care delivery or costs; or
  - For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under the HIPAA regulation is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
    - a. Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
    - b. The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under the HIPAA Privacy regulations.
    - c. The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
    - d. The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

#### **Process for Requesting Exception Determinations - § 160.204**

A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary of HHS. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

1. The State law for which the exception is requested;
2. The particular standard, requirement, or implementation specification for which the exception is requested;
3. The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
4. How health care providers, health plans, and other entities would be affected by the exception;

5. The reasons why the State law should not be preempted by the Federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
6. Any other information the Secretary may request in order to make the determination.

Requests for exception must be submitted to the Secretary of HHS. Until the Secretary's determination is made, the standard, requirement, or implementation specification under the HIPAA Privacy regulations remains in effect. The Secretary's determination will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

#### **Duration of Effectiveness of Exception Determinations - § 160.205**

An exception granted under the HIPAA Privacy regulation remains in effect until:

- a. Either the State law or the Federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
- b. The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

#### **KEY DEFINITIONS**

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **State law** means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.
- **State** refers to one of the following:
  1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan; or
  2. For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.
- **Relates to the privacy of individually identifiable health information** means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.
- **More stringent** means, in the context of a comparison of a provision of State law and a standard, requirement or implementation specification adopted under subpart E of part 164 of the HIPAA regulation, a State law meets one or more of the following criteria:
  1. With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
    - Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with the HIPAA regulation; or
    - To the individual who is the subject of the individually identifiable health information.
  2. With respect to the rights of an individual who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.
  3. With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
  4. With respect to the form, substance, or the need for express legal permission from an individual who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
  5. With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
  6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

- **Contrary**, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:
  1. A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or
  2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

## PROCEDURES

1. If any state laws affect these policies and procedures the Privacy Officer will work with legal counsel to include reference to any such laws in this section.
2. **California** privacy laws outlined here: <http://oag.ca.gov/privacy/privacy-laws>,  
and [https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data\\_breach\\_rpt.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf)  
and <http://www.teenhealthlaw.org/fileadmin/teenhealth/teenhealthrights/ca/CaMinorConsentConfChartFull11-11.pdf>

In California, companies or persons that are the source of a data breach must offer to provide identity theft prevention and mitigation services (if any) to affected individuals **for at least 12 months at no cost** if the breach exposed or may have exposed personal information. The law also expands the range of businesses that are required to implement and maintain security procedures and practices to protect individuals' personal information. Previously, businesses that own or license personal information about California residents were subject to the law, but now businesses that maintain personal information must comply as well. The law maintains that with certain exceptions a person or entity may not sell, advertise for sale, or offer to sell a person's Social Security number. The law went into effect January 1, 2015. A copy of the law can be found at the following web address: [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201320140AB1710&search\\_keywords](http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710&search_keywords).

## POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

## ADDITIONAL RESOURCES

- 45 CFR, Section 160.203-205.
- The Plan's Privacy Officer.
- Useful websites:
  - <http://epic.org/privacy/consumer/states.html>

State Data Breach information:

- [http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data\\_Breach\\_Charts.pdf](http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf)
- <https://www.healthit.gov/policy-researchers-implementers/harmonizing-state-privacy-law>
- <https://oag.ca.gov/privacy/facts/medical-privacy/patient-rights>

# HIPAA PRIVACY POLICY AND PROCEDURE ON NOTIFICATION IN THE CASE OF A BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI)

Effective Date: September 23, 2009, as amended September 23, 2013

---

---

## POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, and 164.414 of the privacy rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

**Effective Date:** The requirements of this policy shall apply with respect to breaches of protected health information occurring **on or after September 23, 2009, as amended September 23, 2013.**

### § 164.404 Notification to Individuals.

1. **Standard-General rule.** A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach.
2. **Breaches treated as discovered.** A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity.
3. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the Federal common law of agency).
4. **Implementation specification: Timeliness of notification.** Except as provided in § 164.412, a covered entity shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
5. **Implementation specifications: Content of notification.**
  - **Elements.** The notification required shall include, to the extent possible:
    - A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
    - C. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
    - D. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
    - E. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
  - **Plain language requirement.** The notification required shall be written in plain language.
6. **Implementation specifications: Methods of individual notification.** The notification required shall be provided in the following form:
  - a. **Written notice.**
    - i. Written notification by **first-class mail** to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
    - ii. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

7. **Substitute notice.** In the case in which there is **insufficient or out-of-date contact information** that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
  - a. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
  - b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:
    - i) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
    - ii) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
8. **Additional notice in urgent situations.** In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice.

#### § 164.406 Notification to the Media.

1. **Standard.** For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.
2. **Implementation specification: Timeliness of notification.** Except as provided in § 164.412, a covered entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
3. **Implementation specifications: Content of notification.** The notification required shall meet the requirements of § 164.404.

#### § 164.408 Notification to the Secretary.

1. **Standard.** A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404, **notify the Secretary.**
2. **Implementation specifications: Breaches involving 500 or more individuals.** For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required contemporaneously with the notice required by § 164.404 and in the manner specified on the HHS web site.
3. **Implementation specifications: Breaches involving less than 500 individuals.** For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches, and not later than 60 days after the end of each calendar year, provide the notification required for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site.

#### § 164.410 Notification by a Business Associate.

1. **Standard.** A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.
2. **Breaches treated as discovered.** For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).
3. **Implementation specifications: Timeliness of notification.** Except as provided in § 164.412, a business associate shall provide the notification required without unreasonable delay and **in no case later than 60 calendar days** after discovery of a breach. Plans may negotiate a tighter notification deadline, such as 30 days or 45 days with a business associate.
4. **Implementation specifications: Content of notification.**

- a. The notification required shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
- b. A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual at the time of the notification required or promptly thereafter as information becomes available.

#### § 164.412 Law Enforcement Delay.

1. **If a law enforcement official states** to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:
  - a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
  - b. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

#### § 164.414 Administrative Requirements and Burden of Proof.

1. **Administrative requirements.** A covered entity is required to comply with the administrative requirements of §§ 164.530(b) (train workforce), (d) (provide a process for individuals to complain), (e) (have and apply appropriate sanctions), (g) (refrain from intimidating or retaliatory acts), (h) (may not require individuals to waive their rights), (i) (must implement policies and procedures to comply with standards), and (j) (change policies and procedures as necessary) with respect to the requirements of this subpart.
2. **Burden of proof.** In the event of a use or disclosure in violation, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach, as defined at § 164.402 (*see Key Definitions below*).

#### KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

#### § 164.402 Definitions.

**Breach means** the acquisition, access, use, or disclosure of (unsecured) protected health information (PHI) in a manner not permitted under subpart E of the HIPAA privacy regulations which compromises the security or privacy of the protected health information (*Note: The HIPAA Privacy Rule is contained in Subpart E. Subpart E extends from §164.500 through §164.534*).

- For an incident or breach investigation prior to September 23, 2013, for purposes of this definition, **compromises the security or privacy of the protected health information** means poses a **significant risk of financial, reputational, or other harm to the individual**. See below for an incident or breach investigation on or after September 23, 2013.
- A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth and zip code does not compromise the security or privacy of the protected health information.

#### **Breach excludes:**

- **Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate**, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
- **Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate**, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
- **A disclosure of protected health information where a covered entity or business associate has a good faith belief** that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

For an incident or breach investigation **on or after September 23, 2013:**

If a violation does not fit into one of the three exclusions noted above, the Privacy Officer will presume that a breach of unsecured PHI has occurred unless a risk assessment, conducted in accordance with these procedures, determines that there is a low probability that the PHI has been compromised. If the Privacy Officer determines there has been a breach of unsecured PHI, the Plan will provide notification in accordance with these procedures.

**Unsecured protected health information means** protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS (in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS web site). At this time, the HHS-specified technologies and methodologies to **secure PHI** are:

- a. **Encryption for electronic PHI** “in motion,” “at rest,” and “in use.” The Plan’s encryption policies are described in its HIPAA Security Policies and Procedures.
- b. **Destruction by shredding** for hardcopy PHI, whether documents, discs, tapes, flash drives or any other portable technology. Electronic PHI is destroyed in accordance with the applicable guidance issues by HHS. The Plan’s Security Policies/procedures describe its procedures for the destruction of electronic PHI, if any.

**Health information** means any information, including genetic 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.

## PROCEDURES

1. All members of the Plan’s workforce are required to report (to the Plan’s Privacy Officer) any use or disclosure of PHI that might be a violation of the Plan’s privacy policies and procedures.

Reports may be made orally or in writing, but must be provided immediately upon committing any action that the person believes may have violated the Plan’s privacy policies and procedures or immediately upon learning that another member of the workforce or any other person (such as a Business Associate) may have done something that may be in violation of the Plan’s privacy policies and procedures.

2. The Privacy Officer will:
  - a) Accept reports from any person who believes there may have been a violation of the Plan’s privacy policies and procedures. If the incident or breach occurred by a Business Associate or its agents/subcontractors, the Privacy Officer will obtain a copy of the most current Business Associate contract with the Plan to review if there are unique provisions about how an incident or breach is to be managed that will need to be considered in addition to Federal law requirements and the process outlined in these procedures. For instance, sometimes the BA contract requires the BA to report an incident or breach to the Plan in less than the legally allowed 60 day period;
  - b) Investigate the alleged violation of the Plan’s privacy policies and procedures, (including reviewing the “policy statement” section at the beginning of this document). We will use the sample HIPAA Incident Report/Risk Assessment form attached to this policy/procedure as a way to organize the information collected during the incident investigation (refer to step 2-g below);
  - c) Question the person or workforce member reporting the perceived violation;
  - d) Question the workforce member or other person who is alleged to have violated the Plan’s privacy policies and procedures;
  - e) Question other persons or workforce members who may have information about the alleged violation;
  - f) Determine, in consultation with other workforce members (and the Plan’s professional advisors, as appropriate), whether there has been a breach of unsecured PHI, as defined in the Plan’s Breach Notification Policy Statement and in the regulations, Section 164.402 (meaning there has been an acquisition, access, use or disclosure of PHI not permitted by the privacy rule that has compromised the security or privacy of the PHI).
    - ✓ **Prior to September 23, 2013**, the determination may require a **risk assessment** of whether the incident poses a significant risk of financial, reputational, or other harm to the individual who is the subject of the PHI; and
    - ✓ **On or after September 23, 2013**, the Privacy Officer will presume that a breach of unsecured PHI has occurred unless the risk assessment that the Privacy Officer performs, conducted in accordance with these procedures, determines that there is a low probability that the PHI has been compromised; and

**On or after September 23, 2013 PRESUME ALL HIPAA INCIDENTS ARE A BREACH until proven otherwise. The burden is on the Plan, the covered entity, or the Business Associate to show that no breach occurred.**

- g) Make and keep a written record of the HIPAA incident investigation (see sample form attached to this policy/procedure) and of the determination whether there has or has not been a breach of unsecured PHI.
3. If the Privacy Officer may have been responsible (or partly responsible) for an incident that may be or is a breach of unsecured PHI, the incident will be investigated by an alternate designee (the Director of Human Resources) and this designee will make the determination whether there has been a breach requiring notification.
4. Legal counsel (the City's attorney's office) may need to be contacted to assist with determining if the incident is truly a breach and for guidance on the need to address identity theft protection in the breach notification letters. Privacy Officer to review the Federal Trade Commission (FTC) educational information in the "Additional Resources" section listed at the bottom of this policy/procedure to determine if the breach notification letters should offer information on the topic of identity theft.
5. The Privacy Office will save the documentation of this research and risk assessment process regardless of whether the outcome of the research shows that the incident is or is not a breach.
6. The Privacy Officer will complete the Plan's HIPAA Incident Log in order to track both non-breach incidents and true breach situations.

#### **Notification to an Individual of a Breach of Unsecured PHI**

1. The Plan will, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been – or is reasonably believed to have been – accessed, acquired, used or disclosed as a result of the breach.
2. The Plan will provide the notice to each individual without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
  - Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.
3. The individual notices will be in writing, in plain language, and will include, to the extent possible, all of the following points:
  - a) A brief description of what happened (including the date of the breach and the date of the discovery of the breach, if known);
  - b) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved) – without listing the actual individual identifiers or other sensitive information involved;
  - c) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
  - d) A brief description of what the Plan is doing to (i) investigate the breach, (ii) mitigate harm to the individual, and (iii) protect against further breaches; and
  - e) Contact information for individuals to ask questions or learn information, including a toll-free phone number, an e-mail address, a Web site, or postal address.
4. The Plan will mail these notices by first-class mail to the individual's last known address. The notification may be provided in one or more mailings as information is available.
  - Or, if the individual agrees to electronic notice and such agreement has not been withdrawn, the Plan will provide the notice by electronic mail.
  - If the Plan knows the individual is deceased and has the address of next of kin or personal representative, the notice will be mailed to that person.
  - If the individual affected by breach is a minor or otherwise lacks legal capacity due to a physical or medical condition, the Plan will provide the notice to the individual's personal representative (who, in the case of a minor child, will typically be the child's parent).
  - If the Plan has insufficient or out-of-date contact information for fewer than 10 individuals, the Plan will use an alternate form of notice such as telephone.

- If the Plan has insufficient or out-of-date contact information for 10 or more individuals, the Plan will notify those individuals either through a conspicuous posting on the Plan's Web site (if any) for a period of 90 days or in appropriate major print or broadcast media.
- **Urgent Situation:** In situations deemed urgent by the Plan due to the possible imminent misuse of unsecured PHI, the Plan may provide notice to the affected individual(s) by phone or other means, in addition to providing the individual written notice.

#### **Notification to the Secretary of Health and Human Services (HHS)**

1. For breaches of unsecured PHI that involve fewer than 500 individuals, the Plan will keep a log and report these breaches to HHS on an annual basis. The reporting of breaches to HHS will occur not later than 60 days after the end of each calendar year in which the breach was discovered by the Plan, and will be performed in the manner specified on the HHS Web site. The Plan may opt to report breaches to HHS at the same time it sends notices to individuals, in the manner specified on the HHS web site.
2. For breaches of unsecured PHI involving 500 or more individuals, the Plan will notify HHS at the same time it provides the individual notices required above, and the reporting will be performed in the manner specified on the HHS Web site.
3. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.
4. HHS Website is located at:  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

#### **Notification to the Media For Breaches Involving 500+ Individuals**

1. For breaches involving more than 500 residents of one state or one jurisdiction (*i.e.*, a geographic area smaller than a state, such as a county, city or town), the Plan will notify prominent media outlets serving the state or jurisdiction at the same time it provides the individual notices required above. The notification to media outlets will be in the form of a press release.
2. The Plan will provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The Plan must notify the media directly and not by posting the notification on its website. The Plan is not required to incur any cost to print or run a media notice.
3. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.

#### **Breach by Business Associate (BA) or Subcontractor of a Business Associate**

1. Through its Business Associate agreements or otherwise, the Plan will require its Business Associates to promptly notify the Plan of any breach of unsecured PHI for which the Business Associate or one of its agents/subcontractors is or may be responsible. The notice will occur without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
2. Through its Business Associate agreement or otherwise, the Plan will determine whether any required notices will be provided by the Plan or by the applicable Business Associate.
  - a. The Business Associate notification required will include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach.
  - b. The Business Associate will provide the Plan with any other available information that the Plan is required to include in notification to the individual at the time of the notification required or promptly thereafter as information becomes available.

#### **Law Enforcement Delay**

1. If a law enforcement official states to the Plan, or the Plan's Business Associate, that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, the Plan will:
  - a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
  - b. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

## **Documentation of an Incident or Breach**

1. The Plan will maintain documentation sufficient to demonstrate that
  - a. for each incident, (1) the requisite investigation and/or risk assessment was conducted and (2) that all required notifications were provided; or
  - b. the use or disclosure at issue did not constitute a breach of unsecured PHI (and thus no notifications were required).
2. The Privacy Officer will retain documentation in accordance with the Plan's Record Retention policy.

## **POLICY/PROCEDURE VIOLATION**

Refer to the Policy on Sanctions.

## **ADDITIONAL RESOURCES**

- 45 CFR, Sections 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, and 164.414.
- The Plan's Privacy Officer.
- HHS website: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>
- FTC website on identity theft: <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>
- FTC educational resources on identity theft: <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>
- Information on Identity Theft Monitoring Services including credit monitoring, fraud alert, security freeze: <http://consumersunion.org/pdf/SecurityFreeze-Consider.pdf> and <http://www.consumerreports.org/cro/news/2014/02/should-you-put-a-security-freeze-on-the-credit-file/index.htm> and <http://learn.equifax.com/credit/fraud-alerts/>
- NIST Special Publication Security Incident Guidance 800-61: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- State Data Breach information: [http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data\\_Breach\\_Charts.pdf](http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf)
- IRS Announcement 2015-22 on taxing identity protection services: <http://www.irs.gov/pub/irs-drop/a-15-22.pdf>

**CITY OF STOCKTON**

**HIPAA INCIDENT REPORT/RISK ASSESSMENT**

The following incident report is an example only and is meant to be customized by our organization. We may find it helpful to give each incident a number. Referring to the incident by number is one more way to help protect the PHI of the person(s) involved in the incident.

- *Pale yellow shaded cells* are data elements similar to what is requested on the HHS website. At a minimum the group health plan must gather data for these yellow shaded cells.

**Incident Number:** \_\_\_\_\_

HIPAA INCIDENT REPORT	
Facts Needed	Information
Date of Report	
Time of Report	
Name of Person Making the Incident Report (First and Last name)	
Title/Position	
Phone numbers (work, cell)	
Work e-mail address	
Location of Incident <i>(these reasons mirror the HHS website)</i>	<input type="checkbox"/> Laptop <input type="checkbox"/> Desktop Computer <input type="checkbox"/> Network Server <input type="checkbox"/> E-mail <input type="checkbox"/> Other Portable Electronic Device <input type="checkbox"/> Electronic Medical Record <input type="checkbox"/> Paper <input type="checkbox"/> Other: _____
Date of Incident	
Time of Incident	
Date of Discovery of the Incident	
Describe the nature of the incident that may have compromised PHI (e.g. Type of protected health information, location of breach, how the breach occurred, amount of health information, circumstances, people involved, etc.)	
Classify the Type of Incident <i>(these reasons mirror the HHS website)</i>	<input type="checkbox"/> Theft <input type="checkbox"/> Loss <input type="checkbox"/> Improper Disposal <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Hacking/IT Incident <input type="checkbox"/> Other: _____ <input type="checkbox"/> Unknown

HIPAA INCIDENT REPORT	
Facts Needed	Information
Type of PHI involved in the breach?  <i>(these reasons mirror the HHS website)</i>	<input type="checkbox"/> Demographic Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clinical Information <input type="checkbox"/> Other: _____
Was PHI compromised in the incident?	
Was PHI actually acquired or viewed by someone not permitted to have access to PHI?	
Who owned the PHI that may have been compromised?	
Who may have impermissibly RELEASED the PHI?	
Who impermissibly USED the PHI?	
Address the Extent of the PHI Involved: <ul style="list-style-type: none"> <li>• How many individuals were impacted by the incident that may have compromised PHI?</li> <li>• What types of identifiers were involved (SSN, name, birthdate, etc.)</li> </ul>	
What has been in place, prior to this incident, to prevent such an incident from happening?	
Have adequate steps been taken to contain the risk and keep it from happening again (mitigate the risk)?	
Does this incident involve a Business Associate of the Plan and/or an agent or subcontractor of the BA?  <i>(If so, indicate name of BA, address, contact person at BA along with contact's phone number and e-mail address)</i>	
Name, phone and e-mail of other people aware of the Incident <i>(list all that apply)</i>	
Was the PHI returned prior to being accessed for improper purposes?	

HIPAA INCIDENT REPORT	
Facts Needed	Information
Does the incident appear to be able to fit one of the permissible EXCEPTIONS to having to call the incident a breach? Best to consult with legal counsel here.	
Safeguards (protective measures) in Place PRIOR TO the Incident	<input type="checkbox"/> Firewalls <input type="checkbox"/> Packet Filtering (router-based) <input type="checkbox"/> Secure Browser Sessions <input type="checkbox"/> Strong Authentication <input type="checkbox"/> Encrypted Wireless <input type="checkbox"/> Physical Security <input type="checkbox"/> Logical Access Control <input type="checkbox"/> Anti-virus Software <input type="checkbox"/> Intrusion Detection <input type="checkbox"/> Biometrics <input type="checkbox"/> Encryption <input type="checkbox"/> Other: _____
Does the Plan HIPAA Policy and Procedure manual or Plan forms need to be updated as a result of this incident?	
<b>Actions Taken in Response to Breach:</b> What other steps has the Plan taken to respond to the incident such as noted to the right?	<input type="checkbox"/> Security and/or Privacy Safeguards <input type="checkbox"/> Mitigation <input type="checkbox"/> Sanctions <input type="checkbox"/> Policies and Procedures <input type="checkbox"/> Revised Business Associate contracts <input type="checkbox"/> Other: _____
If PHI was breached, are there steps that affected individuals can/should take to prevent further harm?	
Do staff need additional training as a result of this incident?	
Need for employee sanctions?	
<b>Name of Privacy Officer</b>	
<b>Date Privacy Officer became aware of the incident</b>	
<b>Incident is considered to be a Breach in accordance with breach notification regulations?</b>	<b>Circle One:</b> <b>No</b> <b>Yes</b> (if yes continue to complete rest of form)
Date and Name of Legal Counsel consulted	
Who drafted the Notice that will be sent to affected individuals?	
Date Individual Notice(s) mailed/provided	
Was a Substitute Notice required?	<input type="checkbox"/> No <input type="checkbox"/> Yes
Was a Media Notice required?	<input type="checkbox"/> No <input type="checkbox"/> Yes
Date breach log completed if less than 500 individuals affected	

HIPAA INCIDENT REPORT	
Facts Needed	Information
Date HHS website breach reporting form completed online, if 500 + individuals affected	
Date media contacted if 500+ individuals affected?	
Date of group health plan or IT department staff training or retraining related to this breach. List who taught the training and attach attendance list of who attended the training.	

*Once completed, please return this form to the:*  
**City of Stockton Deputy Director of Human Resources – Risk & Benefits**  
 400 E. Main Street, 3<sup>rd</sup> Floor Stockton CA, 95202  
 Telephone: 209-937-8233      Confidential fax #: 209-937-5702

## CITY OF STOCKTON

### CHECKLIST FOR CREATION OF AN INDIVIDUAL BREACH NOTICE

*When the Plan creates its Notice to an Individual, the Plan will be sure EACH notice contains EACH of the following **required elements**. The Plan will retain proof of the notices distributed.*

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); without listing the actual individual identifiers or other sensitive information involved,
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to (a) investigate the breach, (b) to mitigate harm to individuals, and (c) to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, Web site, or postal address.
- Assurance that the notice is written in plain language.

Our organization **may include** other customized information in the breach notification letter, including:

- •Consumer advice directing the individual to review account statements and monitor credit reports
- •Recommendations that the individual place a fraud alert on their credit card accounts, or contact a credit bureau to obtain credit monitoring services, if appropriate
- •Contact information for credit reporting agencies, including the information needed for reports for criminal investigation and law enforcement
- •Contact information for national consumer reporting agencies

## SAMPLE BREACH NOTIFICATION LETTER TEMPLATE

A breach notification letter must be **written in plain language** and include all of the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
- If there is concern for **identity theft**, we will consider reviewing information at this FTC website: <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>

**STOP AND CUSTOMIZE AT THE BRACKETED AREAS [ ] and double check once letter drafted that it still includes all the required components as noted above.**

**Legal counsel is to review any draft breach notification letter to plan participants.**

**Remember to do the required HHS online notification too.**

[Date]

[Name ]

[Address]

[City, State Zip Code]

Dear [Name of Person]:

I am writing to you with important information about a recent [unauthorized disclosure/access/posting, etc.] of your personal information from [Name of Covered Entity (CE) or Business Associate (BA)].

### **Brief Description of Incident**

The following outlines a brief description of the facts of the incident: \_\_\_\_\_.  
The types of unsecured protected health information that were involved in the incident included: (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

We became aware of this event on [Insert Date] and [believe] [after investigation have discovered that] the incident occurred on [or about] [Insert Date].

### **Steps We Have Taken**

We take the privacy and security of your protected health information very seriously. We have taken the following steps:

*Insert a brief description of what the CE or BA is doing to investigate the breach, to mitigate potential harm to individuals, and to protect against further breaches such as reporting to appropriate authorities, reviewing policies, audit and monitoring, re-education, employee disciplinary action, etc.*

## Steps You May Need To Take

We recommend that you:

*Insert any steps the individual should take to protect themselves from potential harm resulting from the breach such as notifying their health insurance company, changing your account numbers, notifying credit monitoring agencies, \_\_\_\_\_, etc. See the Optional Content area of this letter for wording ideas.*

### For Additional Information Contact

*Insert contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.*

We sincerely regret that this [*insert event, such as loss*] of protected health information has occurred and wish to assist you with questions you may have. If you need additional information please contact \_\_\_\_\_, (toll-free) at: ( ) \_\_\_\_-\_\_\_\_\_.

### Optional Content

*You may decide to offer credit monitoring services in addition to contact information for credit agency fraud reporting.*

To help ensure that this information is not used inappropriately, [Name of CE/ BA] will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [Need to document the process for how this would work].

We also advise you to immediately take the following steps:

- **Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report.** This can help prevent an identity thief from opening additional accounts in your name. As soon as a credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report through their bureau too, and all three credit reports will be sent to you free of charge.

***Always verify these phone numbers, addresses and websites before mailing letters in case these agencies change this information:***

- ✓ **Equifax:** 1-800-525-6285 or 1-888-766-0008; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241.
- ✓ **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013.
- ✓ **TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

- **Order your credit reports.** By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- **Continue to monitor your credit reports.** Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.
- [If concerned about Identity Theft issues, review the consumer information at this website: <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>]

## **Closing Statement**

While we are uncertain whether your personal information was actually obtained, we want to bring this situation to your attention. We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. We offer our sincerest apology for this [situation] [unfortunate incident] and we are taking appropriate measures to prevent a reoccurrence.

[With my sincere apology] *or* [Sincerely],

*[Insert Applicable Name/Contact Information, often the Privacy Officer or Security Officer]*

Privacy Officer for \_\_\_\_\_



# HIPAA PRIVACY POLICY AND PROCEDURE ON LIMITATIONS ON THE USE AND DISCLOSURE OF GENETIC INFORMATION

Effective Date: September 23, 2013

---

---

## POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(a)(5)(i) under the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Non-Discrimination Act of 2008. If the privacy rules are changed by HHS, the Plan will follow the revised rules.

## LIMITATIONS ON USE AND DISCLOSURE OF GENETIC INFORMATION POLICY

The Plan will not use or disclose PHI that is genetic information for underwriting purposes. Genetic information includes, with respect to an individual, information about:

- The individual's genetic tests;
- The genetic tests of the individual's family members;
- The manifestation of a disease or disorder in family members (described below) of such individual; or
- Any request for, or receipt of, genetic services, or participation in clinical research, which includes genetic services, by the individual or any family member (described below) of the individual.

References to "**family members**" include: parents, spouses, siblings, children, grandparents, grandchildren, aunts, uncles, nephews, nieces, great-grandparents, great-grandchildren, great aunts, great uncles, first cousins, great-great grandparents, great-great grandchildren and children of first cousins, whether by consanguinity (such as siblings who share both parents) or affinity (such as by marriage or adoption).

In addition, references to **genetic information of an individual or family member** includes the genetic information of a fetus carried by the individual or family member, and any embryo legally held by an individual or family member using assisted reproductive technology.

*Examples of prohibited use and disclosure of PHI that is genetic information for underwriting:*

- *A health insurance company uses an individual's family medical history or genetic test result, that was in the group health plans claims experience, to adjust the plan's blended, aggregate premium rate for the new plan year.*
- *A group health plan uses an individual's family medical history that was provided as part of a health risk assessment, to provide a premium reduction to the individual. It would be permissible to request family medical history through a health risk assessment that is completed after enrollment or is unrelated to the group health plan enrollment and that is not tied to any reward or penalty.*

## KEY DEFINITIONS

- **Underwriting purposes** is defined broadly to include:
  - Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of coverage for, benefits under the Plan. Among other items, this includes changes in deductibles or other cost sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program;
  - The computation of premium or contribution amounts under the Plan. Among other items, this includes discounts, rebates, payment in kind or any other premium differential mechanisms in return for completing a health risk assessment or participating in a wellness program;
  - If applicable, the application of any pre-existing condition exclusion under the Plan; and
  - Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

Underwriting purposes **do not include** determinations of medical appropriateness where an individual seeks a benefit under the Plan.

- **In Kind** refers to being paid or given goods, commodities, or services instead of money.

- **Genetic information** means:
  1. Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
    - i. The individual's genetic tests;
    - ii. The genetic tests of family members of the individual;
    - iii. The manifestation of a disease or disorder in family members of such individual (*manifestation defined below*); or
    - iv. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
  2. Any reference to genetic information concerning an individual or family member of an individual shall include the genetic information of:
    - i. A fetus carried by the individual or family member who is a pregnant woman; and
    - ii. Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
  3. Genetic information excludes information about the sex or age of any individual.
- **Genetic services** means:
  1. A genetic test;
  2. Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
  3. Genetic education.
- **Genetic test** means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.
- **Manifestation or manifested** means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. A disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

## PROCEDURES

1. The Plan will not use genetic information, or request that its Business Associates use genetic information, for underwriting purposes (as that term is defined above).
2. See also the policy/procedure in this Manual on Fundraising and Underwriting.

## POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions and the Policy on Fundraising and Underwriting.

## ADDITIONAL RESOURCES

- 45 CFR, Section 164.502(a)(5)(i).
- The Plan's Privacy Officer.

5313838v3/00479.004