



---

# City Policies

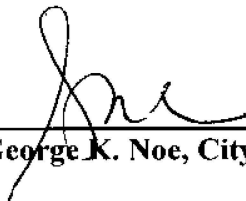
---

SUBJECT: Health Insurance Portability & Accountability Act  
(HIPPA) Privacy Policies & Procedures

NO. HR 29.0

Effective: 04/14/2003  
Revised: 01/17/2005

APPROVED:

  
\_\_\_\_\_  
George K. Noc, City Manager

EFFECTIVE: 1-18-05

## TABLE OF CONTENTS

|   | <b>Page</b> |
|---|-------------|
| I. GENERAL ADMINISTRATIVE POLICIES AND PROCEDURES .....   | 1           |
| A. General Guidelines.....  | 1           |
| B. Designation of a Privacy Officer and Assistant Privacy Officer .....                                 | 3           |
| C. Development and Maintenance of Privacy Policies and Procedures.....                                  | 5           |
| D. Safeguards for Protected Health Information .....  | 6           |
| E. Refraining from Intimidating or Retaliatory Acts .....   | 7           |
| F. No Waiver of Rights .....  | 8           |
| G. Informing Workforce of the Need for Confidentiality .....  | 9           |
| H. Workforce Training Regarding the Use and Disclosure of Protected Health Information .....            | 11          |
| II. REQUIREMENTS FOR GROUP HEALTH PLANS.....  | 13          |
| III. FIREWALLS: CREATION OF AN ADEQUATE SEPARATION OF THE GROUP HEALTH PLANS FROM THE PLAN SPONSOR..... | 16          |
| A. Adequate Separation Between the Group Health Plans and the Plan Sponsor .....                        | 16          |
| B. Authority and Responsibility of Individual Workforce Members.....                                    | 18          |
| C. Allocation of Job Tasks for PHI-Related Functions .....  | 19          |
| IV. IDENTIFYING WHEN ROUTINE HEALTH INFORMATION BECOMES PHI .....                                       | 22          |
| A. Determination of PHI Status.....   | 22          |
| B. Creating De-Identified Information .....   | 24          |
| C. Limited Data Sets.....   | 27          |
| V. TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS.....   | 30          |
| A. Disclosure of PHI for Treatment, Payment, and Health Care Operations .....                           | 30          |
| B. Disclosure of PHI for Treatment Purposes .....   | 32          |
| C. Disclosure of PHI for Payment Purposes.....  | 33          |
| D. Disclosure of PHI for Health Care Operations .....   | 35          |
| E. Incidental Disclosures of PHI .....  | 37          |
| F. Treatment of Protected Health Information After Death.....   | 38          |
| VI. THE MINIMUM NECESSARY STANDARD.....   | 39          |
| A. Disclosing and Requesting Only the Minimum Amount of PHI Necessary .....                             | 39          |

**TABLE OF CONTENTS**  
(continued)

|  | <b>Page</b> |
|--|-------------|
| VII. DISCLOSURES TO PERSONS WITH A RELATIONSHIP TO AN INDIVIDUAL.....                              | 43          |
| A. Personal Representatives .....  | 43          |
| B. Using PHI for Involvement In and Notification of the Individual's Care.....                     | 45          |
| VIII. REQUIRED DISCLOSURES OF PHI UNDER HIPAA.....   | 47          |
| IX. PERMITTED DISCLOSURES UNDER HIPAA .....  | 48          |
| A. Disclosing PHI as Required by Law .....   | 48          |
| B. Disclosing PHI for Public Health Release .....  | 51          |
| C. Disclosing PHI about Victims of Abuse, Neglect, or Domestic Violence .....                      | 54          |
| D. Disclosing PHI for Health Oversight Release .....   | 56          |
| E. Disclosing PHI for Judicial and Administrative Release.....                                     | 59          |
| F. Disclosing PHI for Law Enforcement Release .....  | 62          |
| G. Disclosing PHI about Decedents .....  | 65          |
| H. Disclosing PHI for Cadaveric Organ, Eye, or Tissue Donation .....                               | 67          |
| I. Disclosing PHI to Avert Serious Threat to Health and Safety.....                                | 69          |
| J. Disclosing PHI for Specialized Government Functions .....                                       | 72          |
| K. Disclosing PHI for Worker's Compensation.....   | 75          |
| X. VERIFICATION OF INDIVIDUALS OR ENTITIES REQUESTING USE OR DISCLOSURE OF PHI .....               | 77          |
| XI. AUTHORIZATIONS .....   | 79          |
| A. Authorization to Use or Disclose PHI .....  | 79          |
| B. Conditioning Services or Eligibility on the Provision of an Authorization to Disclose PHI ..... | 81          |
| C. Individual Revocation of an Authorization to Disclose PHI .....                                 | 82          |
| D. Prohibiting the Use of an Invalid Authorization to Disclose PHI .....                           | 83          |
| E. Authorization for the Use or Disclosure of Psychotherapy Notes.....                             | 84          |
| XII. NOTICE OF PRIVACY PRACTICES.....  | 86          |
| A. Content of Notice.....  | 86          |
| B. Provision of Notice of Privacy Practices .....  | 90          |
| XIII. BUSINESS ASSOCIATES .....  | 92          |
| A. Relationships with Business Associates .....  | 92          |

## TABLE OF CONTENTS

(continued)

|  | <b>Page</b> |
|--|-------------|
| B. Investigation and Correction of Business Associate Contractual Breaches .....                           | 94          |
| C. Reporting of Contractual Breaches by Business Associates.....   | 95          |
| XIV. POLICY ON USE OF PHI FOR MARKETING .....  | 96          |
| XV. INDIVIDUALS' RIGHTS UNDER HIPAA .....  | 98          |
| A. Requesting Restrictions on Uses and Disclosures .....   | 98          |
| B. Requests for Confidential Communications for PHI.....   | 100         |
| C. Effective: April 14, 2003 .....   | 100         |
| D. Granting Access to Inspect and Obtain a Copy .....  | 102         |
| E. Denying Access to Inspect and Obtain a Copy of PHI.....   | 105         |
| F. Reviewing a Denial to Access PHI.....   | 108         |
| G. Accepting Requests for Amendments to PHI.....   | 110         |
| H. Denying Requests for Amendments to PHI.....   | 113         |
| I. Accounting of Disclosures.....  | 116         |
| J. Individual Rights to File Complaints.....   | 119         |
| XVI. SANCTIONING OF WORKFORCE.....   | 120         |
| XVII. MITIGATION OF VIOLATIONS .....   | 123         |
| XVIII. MAINTAINING APPROPRIATE DOCUMENTATION REGARDING<br>COMPLIANCE WITH HIPAA PRIVACY REQUIREMENTS ..... | 124         |

# I. GENERAL ADMINISTRATIVE POLICIES AND PROCEDURES

## A. General Guidelines

**Effective: April 14, 2003**

The City of Corpus Christi ("Employer" or "Plan Sponsor") maintains certain group health plans for the benefit of its employees and their dependents. The policies and procedures set forth in this manual establish the administrative procedures of the group health plans maintained by the Employer for safeguarding the privacy of protected health information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in relation to such group health plans (the "Covered Entity").

Except to extent specifically stated otherwise, the policies and procedures set forth in this manual govern the operation of the following group health plans maintained by the Employer under the HIPAA privacy regulations:

The City of Corpus Christi – Citicare Employee Benefit Plan

The City of Corpus Christi – Citicare Public Safety Employee Benefit Plan

The City of Corpus Christi – Citicare Fire Employee Benefit Plan

The City of Corpus Christi – Citicare Basic Care Employee Benefit Plan

The City of Corpus Christi Dental Plan

The City of Corpus Christi Vision Plan

The Medical Expense Flexible Reimbursement Account under the City of Corpus Christi Cafeteria Plan

The group health plans listed above are hereby designated as part of an Organized Health Care Arrangement ("OHCA") and shall be subject to the same policies and procedures as set forth in this manual. As an OHCA, such group health plans shall provide a joint notice to applicable group health plan participants. The self-insured group health plans listed above shall be collectively referred to throughout this manual as the "**OHCA Members**".

The Plan Sponsor maintains the following fully-insured group health plans:

The City of Corpus Christi Vision Benefits Plan (insured by LifeRe Insurance Co.)

The City of Corpus Christi Critical Care Plan (insured by AFLAC)

The City of Corpus Christi Long-Term Care Plan (insured by Unum)

The Plan Sponsor has determined that it will not receive protected health information from the insurance carrier except as specifically permitted under 45 CFR 164.504(f)(1)(ii). The Plan Sponsor shall only receive Summary Health Information and information relating to enrollment and participation in a group health plan. Thus, the fully-insured health plans listed above will not be subject to the rules as set forth in this manual and the insurance carrier for each such plan shall be responsible for complying with HIPAA's privacy rules in relation to such plans. Pursuant to 45 CFR 164.530(k), the Plan Sponsor shall only be responsible for 1) refraining from intimidating or retaliatory acts, 2) refraining from requiring a waiver of HIPAA rights as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits and 3) maintaining a copy of the plan documents for six years in relation to the fully-insured plans listed above.

## **B. Designation of a Privacy Officer and Assistant Privacy Officer**

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.530(a) requires the designation of a Privacy Officer responsible for policy development and handling of privacy inquiries and complaints. The Privacy Officer shall safeguard the privacy of protected health information consistent with federal and state law and regulations thereunder. OHCA Members are committed to ensuring the privacy and security of protected health information. In order to manage the facilitation and implementation of activities related to the privacy and security of protected health information, OHCA Members will appoint and maintain an internal Privacy Officer position. The Privacy Officer will be trained on all policies and procedures necessary to fulfill his or her responsibilities in ensuring the security and privacy of protected health information. An Assistant Privacy Officer will be designated by the Privacy Officer to assist in the oversight of the policies and procedures set forth in this manual and to serve as an initial contact person responsible for providing further information and receiving complaints about privacy practices.

### **Policy**

1. OHCA Members will designate a Privacy Officer responsible for oversight of the policies and procedures regarding the privacy of health information. Privacy Officer will designate an Assistant Privacy Officer to assist the Privacy Officer and to serve as an initial contact person for providing further information and receiving complaints about privacy practices.
2. The Health Benefits Manager shall be appointed as the Privacy Officer of the OHCA Members. The Privacy Officer shall appoint the Assistant Privacy Officer. The Assistant Privacy Officer shall be the Senior Management Assistant in HR.

### **Procedures**

1. The Privacy Officer shall safeguard the privacy of protected health information and shall be responsible for the development and oversight of the policies and procedures set forth in this manual.
2. The Privacy Officer shall be responsible for policy development and handling privacy inquiries and complaints.
3. The Privacy Officer will be trained regarding policies and procedures for safeguarding protected health information and shall be responsible for the OHCA Members' compliance with such policies and procedures, including:
  - (a) the secure transmission and storage of individual health information in any form;
  - (b) the control of access to individual health information;

- (c) the secure management of protected health information;
  - (d) the proper use and disclosure of protected health information at the request of the individual;
  - (e) the proper use and disclosure of protected health information without the authorization of the individual;
  - (f) authorizations regarding the use or disclosure of protected health information;
  - (g) individual rights regarding protected health information;
  - (h) the negotiation and maintenance of contracts with business associates regarding the use and disclosure of protected health information;
  - (i) the proper distribution of the notice of privacy practices;
  - (j) the investigation and correction of violations of privacy policies and procedures;
  - (k) audits for compliance with the privacy policies and procedures;
  - (l) the maintenance of records regarding access to individual health information;
  - (m) the receipt of questions from workforce members and individuals concerning privacy practices and procedures.
4. Training will be conducted as early as possible within the first year of the Privacy Officer's employment with Plan Sponsor. Training will incorporate the unique specifications and implications of Plan Sponsor's routine business activities.
  5. The Privacy Officer may assign any of these responsibilities to other staff members, including an Assistant Privacy Officer, but will continue to have overall responsibility for making sure the policies and procedures set forth in this manual are carried out in accordance with HIPAA.
  6. An Assistant Privacy Officer will be designated by the Privacy Officer to assist in the oversight of the policies and procedures set forth in this manual and to serve as an initial contact person responsible for providing further information and receiving complaints about privacy practices.



## **C. Development and Maintenance of Privacy Policies and Procedures**

**Effective April 14, 2003**

### **Purpose**

45 CFR 160.530(i)(1) requires covered entities to establish written policies and procedures to implement HIPAA's privacy standards.

### **Policy**

The Privacy Officer shall be responsible for establishing written policies and procedures governing the OHCA Members' use and disclosure of protected health information. The OHCA Members retain the right to periodically amend such policies and procedures from time to time.

### **Procedure**

1. The Privacy Officer will develop policies and procedures that are designed to comply with HIPAA's privacy regulations.
2. The Privacy Officer will monitor changes in the law and regulations that may require modifications to the policies and procedures set forth in this manual. The Privacy Officer shall be responsible for developing new or revised policies and procedures as necessary to comply with revisions to the law. The Privacy Officer shall also determine whether the Notice of Privacy Practices must be revised to reflect the new or revised privacy policies and procedures. The effective date of a revised policy or procedure must not be earlier than the date on which the revised Notice of Privacy Practices is made available to affected individuals.
3. The Privacy Officer may initiate amendments to the policies and procedures as required by law or as desired by the OHCA Members.
4. All policies and procedures and any amendments thereto must be approved by the City Manager of the City of Corpus Christi.
5. The Privacy Officer shall announce the adoption of new or revised policies or procedures by any means reasonably anticipated to reach all workforce members affected by such change. Such communication shall describe the new policy, indicate its effective date and indicate when and where the new policy or procedure will be available for review.
6. If any material revisions are made to the policies and procedures, the Privacy Officer shall require training of all workforce members affected by such revisions within a reasonable time after the adoption of such revisions.

## **D. Safeguards for Protected Health Information**

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.530(c) requires covered entities to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the privacy rule.

### **Policy**

It is the policy of OHCA Members to implement reasonable administrative, technical and physical safeguards to protect the privacy of protected health information.

### **Procedures**

1. OHCA Members will reasonably safeguard protected health information from all intentional and unintentional uses or disclosures in violation of the privacy rule. OHCA Members will also reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use of disclosure.
2. OHCA Members shall take all reasonable precautions to abide by the policies and procedures set forth in this manual.
3. OHCA Members shall ensure that all reasonable technical safeguards have been put in place to protect the privacy of protected health information, including but not limited to firewalls, restricted computer access, and computer passwords.
4. OHCA Members shall ensure that reasonable physical safeguards are implemented to ensure the privacy of protected health information, including but not limited to the removal of all protected health information from open desk areas when not in use, the use locks on all filing cabinets and desk drawers where protected health information is stored and the prohibition of access of unauthorized individuals to work areas in which protected health information is used or stored unless such individuals are accompanied or monitored by authorized personnel.

## **E. Refraining from Intimidating or Retaliatory Acts**

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.530(g) requires covered entities to not intimidate, threaten, coerce, discriminate against, or take retaliatory action against individuals for exercising any rights provided under the privacy rules.

### **Policy**

It is the policy of OHCA Members to refrain from intimidating or retaliatory acts against individuals for exercising rights provided under the HIPAA privacy rules.

### **Procedures**

1. OHCA Members will not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against:
  - (a) any individual for the exercise of any right under, or for participation by the individual in any process established by the privacy rule, including filing a complaint with OHCA Members or Health and Human Services; or
  - (b) any individual or other person for:
    - filing a complaint with Health and Human Services;
    - testifying, assisting or participating in an investigation, compliance review, proceeding or hearing; or
    - opposing any act or practice made unlawful by the privacy rule, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the privacy rules.
2. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or Assistant Privacy Officer, or to the employee compliance hotline.

## **F. No Waiver of Rights**

**Effective: April 14, 2003**

### **Purpose and Policy**

45 CFR 164.530(h) provides that a covered entity may not require individuals to waive their rights to file complaints to Health and Human Services or their rights under the privacy rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

### **Procedures**

1. OHCA Members shall implement policies and procedures with respect to protected health information designed to comply with the requirements of the privacy rule.
2. OHCA Members will not require individuals to waive their rights to file complaints to Health and Human Services or their rights under the privacy rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
3. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or Assistant Privacy Officer, or to the employee compliance hotline.

## **G. Informing Workforce of the Need for Confidentiality**

**Effective: April 14, 2003**

### **Purpose**

This policy covers all the workforce of OHCA Members and Plan Sponsor. All workforce members are responsible for safeguarding the privacy of protected health information. Specific workforce member responsibilities under these privacy policies and procedures will be listed in the workforce member's job description.

### **Policy**

It is the policy of OHCA Members to maintain the highest level of confidentiality for individuals and employees at all times and under all circumstances.

#### **1. Protected Health Information**

All protected health information is strictly confidential and can be shared only with those who have a "need to know" in the due course of business and operations, and only in a secure area. The "Need to Know" is defined as that which is necessary for one to perform one's specific job responsibilities adequately.

#### **2. Breach of Confidentiality**

- (a) "Carelessness" is defined as a breach that occurs when an employee unintentionally or carelessly accesses, reviews, or reveals protected health information to himself/herself or others without a legitimate need to know the protected health information. Examples include, but are not limited to: employees discussing protected health information in a public area; employees leaving a copy of protected health information in a public area; employees leaving a computer work station unsecured.
- (b) "Curiosity or Concern" is defined as a breach when an employee accesses, reviews, or discusses protected health information for purposes other than the performance of job functions related to the protected health information. Examples include but are not limited to an employee looking up birth dates, addresses of friends or relatives, accessing and reviewing an individual's record out of concern or curiosity; or reviewing a public person's record.
- (c) "Personal Gain or Malice" is defined as a breach when an employee accesses, reviews, or discusses protected health information for personal gain or with malicious intent.

### **Procedure**

- 1. Discovery by a Privacy Officer, the Assistant Privacy Officer or Supervisor

- (a) If a Privacy Officer, Assistant Privacy Officer or supervisor believes a breach has occurred by an employee, after investigation, the OHCA Members' discipline process will be followed (see the Policy and Procedure entitled "Sanctioning of Workforce"). The scope and severity of the outcome will assist in determining what level of disciplinary action is imposed.
  - (b) The incident shall be reported in the employee's personnel file.
- 2. Discovery by a Co-Worker
  - (a) The individual who observes or is aware of a breach of confidentiality shall report it to the Assistant Privacy Officer (unless it is the Assistant Privacy Officer, then it shall be reported to the Privacy Officer).
  - (b) Failure to report a breach of confidentiality will result in disciplinary action.
  - (c) Reporting a breach of confidentiality in bad faith or for malicious reasons will result in disciplinary action.
- 3. All documentation concerning the employee who violates this procedure will be stored in the employee's personnel file.
- 4. Mail
  - (a) Tampering with incoming or outgoing mail, mail which has been placed in the distribution boxes, or any communication contained in a "confidential security envelope," is prohibited.
  - (b) All interdepartmental mail of a confidential nature is to be placed in a secure, confidential envelope and is to be opened only by the addressee.
- 5. Any breaches of confidentiality shall be taken into account for the purpose of imposing sanctions for violations of the privacy rule (see Policy entitled "Sanctioning of Workforce").
- 6. An employee shall maintain the confidentiality of information even after termination of such employee's employment.

## **H. Workforce Training Regarding the Use and Disclosure of Protected Health Information**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. To support our commitment to confidentiality, all workforce members who have access to protected health information in order to perform their job-related functions for OHCA Members will receive appropriate training regarding the policies and procedures for using and/or disclosing protected health information, as required under 45 CFR §164.530(b).

### **Policy**

OHCA Members will train all workforce members who have access to protected health information as part of their job-related functions regarding the proper use and disclosure of protected health information.

### **Procedures**

1. Employee training regarding the use and disclosure of protected health information will include the following:
  - HIPAA's basic principles and the specific requirements set forth in this manual governing the safeguarding of protected health information;
  - the process by which an individual may request the use or disclosure of his or her protected health information;
  - the use and disclosure of protected health information for treatment, payment and health care operations;
  - the process by which OHCA Members may obtain an authorization from an individual to use or disclose his or her protected health information;
  - the right of the individual to revoke an authorization;
  - the identification of defective authorizations; and
  - the penalties and procedures for handling violations of the privacy policies and procedures.
2. Initial training will occur no later than April 14, 2003. Thereafter, training will occur within a reasonable period of time after a new employee's initial employment, and thereafter at the discretion of the Privacy Officer.
3. Training will be provided to all workforce members whose functions are affected by a material change in the policies and procedures as set forth in this manual within a reasonable period of time after the material change becomes effective.
4. OHCA Members will document that training as described in this policy has been completed by all affected workforce members. The documentation of training shall be

performed in accordance with the policies and procedures in this manual addressing HIPAA's documentation requirements.

5. Training will be conducted by the Privacy Officer, the Assistant Privacy Officer or a third party designated by the Privacy Officer.



## **II. REQUIREMENTS FOR GROUP HEALTH PLANS**

### **Purpose**

Pursuant to 45 CFR 164.504(f), in order for a group health plan to disclose protected health information to the Plan Sponsor, the group health plan must ensure that the plan documents restrict uses and disclosures of such information by the Plan Sponsor consistent with the requirements of the privacy rules. This policy is designed to give guidance and to ensure compliance with all laws and regulations regarding the Plan Sponsor's use of protected health information in administering the group health plans covered under HIPAA.

### **Policy**

1. The plan documents of the OHCA Members shall be amended to incorporate the requirements of 45 CFR 164.504(f)(2) before OHCA Members disclose protected health information to the Plan Sponsor.
2. OHCA Members shall require the Plan Sponsor to execute a certification that the plan documents have been amended to incorporate the provisions set forth in 45 CFR 164.504(f)(2)(ii) before disclosing protected health information to the Plan Sponsor.
3. OHCA Members shall ensure the adequate separation between the group health plans and the Plan Sponsor as set forth in 45 CFR 164.504(f)(2)(iii) before disclosing protected health information to the Plan Sponsor.

### **Procedures**

1. OHCA Members shall verify that all group health plan documents have been amended to (1) establish permitted and required uses and disclosures of protected health information by the Plan Sponsor, (2) to require the Plan Sponsor to execute a certification stating that the Plan Sponsor will abide by the requirements of 164.504(f)(2)(ii), and (3) to provide for the adequate separation between the group health plan and the Plan Sponsor before disclosing protected health information to the Plan Sponsor.
2. The Plan Sponsor shall execute a certification stating that the plan documents have been amended and that the Plan Sponsor agrees to:
  - (a) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
  - (b) Ensure that any agents, including subcontractors, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such information;
  - (c) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;

- (d) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
  - (e) Make available protected health information in accordance with 45 CFR 164.524;
  - (f) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with 45 CFR 164.526;
  - (g) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528;
  - (h) Make its internal practices, books and records relating to the use and disclosure of protected health information received from the group health plan available to Health and Human Services for purposes of determining compliance by the group health plan with the privacy rules;
  - (i) If feasible, return or destroy all protected health information received from the group health plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
  - (j) Ensure that adequate separation between the group health plan and the Plan Sponsor has been established.
3. An adequate separation between the group health plan and Plan Sponsor shall be established (*i.e.*, a firewall) in which:
- (a) Those employees or classes of employees or other persons under the control of the Plan Sponsor to be given access to the protected health information to be disclosed are described, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;
  - (b) The access to and use by such employees described in (a) shall be restricted to the plan administration functions that the Plan Sponsor performs for the group health plan; and
  - (c) An effective mechanism for resolving any issues of noncompliance by persons described in (a) is put in place.
4. Upon satisfaction of the steps described above, the group health plans may disclose protected health information to the Plan Sponsor to carry out plan administration functions that the Plan Sponsor performs. The group health plans may not disclose protected health information to the Plan Sponsor for the purpose of employment-related

actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor.

5. All workforce members of Plan Sponsor shall immediately notify the Privacy Officer upon learning of a violation of the privacy rule or the policies and procedures set forth in this manual.

### **III. FIREWALLS: CREATION OF AN ADEQUATE SEPARATION OF THE GROUP HEALTH PLANS FROM THE PLAN SPONSOR**

#### **A. Adequate Separation Between the Group Health Plans and the Plan Sponsor**

**Effective: April 14, 2003**

##### **Purpose**

45 CFR 164.504(f)(2)(iii) requires that an adequate separation must exist between the group health plan and the Plan Sponsor. The Plan Sponsor must not use or disclose any protected health information from the group health plans for the purpose of employment-related actions, any business functions or decisions, or any decisions in connection with any other benefit plan of the Plan Sponsor (such as disability plans, life insurance plans, or workers' compensation plans).

##### **Policy**

OHCA Members shall create a firewall to ensure the adequate separation between the group health plans and the Plan Sponsor.

##### **Procedure**

1. OHCA Members shall implement reasonable measures to ensure the adequate separation of the group health plans from the Plan Sponsor when performing an employer-related function or when making a business decision.
2. OHCA Members shall describe those classes of employees or other persons under the control of the Plan Sponsor to be given access to protected health information.
3. OHCA Members shall restrict the access to and use by such employees and other persons described in Procedure 2 to the plan administration functions that the Plan Sponsor performs for the group health plans.
4. Except for those employees described in Procedure 2, an employee of the Plan Sponsor shall not have access to protected health information at any time, unless an individual has executed an authorization specifically allowing such employee to access, use and/or disclose such individual's protected health information. For example, individuals within the personnel department may not access group health plan information to decide the number of handicapped parking spaces required to be in the employee parking lot. Further, an individual's supervisor may not access group health plan records to determine whether an employee requires special accommodations for a disability.

5. Employees described in Procedure 2 who also perform employer-related functions for the employer (*i.e.*, FMLA and other leave determinations, workers' compensation functions, hiring and termination decisions) are strictly prohibited from using protected health information obtained from group health plan administrative functions for employment-related decisions. All employment-related decisions relating to an individual must be separately and adequately documented in the individual's personnel or other employment records without reference to files maintained in relation to the group health plans covered under the privacy rule.

For example, if an individual approaches a Health Benefits employee who assists in both the operation of the group health plan and FMLA for approval of a leave of absence, such Health Benefits employee must make the FMLA determination without reference to any claims or other information from the group health plan. Justification for the leave must be documented solely from sources other than protected health information from the group health plan. The Health Benefits employee may receive medical information directly from the individual or the individual's physician documenting the reason for the leave of absence. Such medical information will not be considered protected health information for purposes of the privacy rule. Such documentation received for the purpose of determining whether to grant the leave of absence must always be stored separately from group health plan files.

6. OHCA Members shall implement adequate and reasonable safeguards to prevent employees of the Plan Sponsor who are not described in Procedure 2 from accessing protected health information from the group health plans.
7. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **B. Authority and Responsibility of Individual Workforce Members**

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.514(d)(2)(ii) requires reasonable efforts to limit access of workforce members to the classes of information necessary to carry out their duties in relation to the Covered Entity.

### **Policy**

It is the policy of OHCA Members to implement reasonable safeguards to limit access of workforce members to the classes of information necessary to carry out their duties in relation to the Covered Entity.

### **Procedures**

1. The job description of all workforce members who require routine access to protected health information to perform their job-related duties must identify:
  - the job functions that require the use or disclosure of protected health information;
  - the classes of protected health information that the position will use or disclose; and
  - any restrictions on the protected health information that the position can use or disclose.

These requirements may be satisfied by referring to the Policy entitled "Allocation of Job Tasks for PHI-Related Functions" that the Privacy Officer may amend from time to time to define the positions authorized to routinely use or disclose standard categories of protected health information.

## C. Allocation of Job Tasks for PHI-Related Functions

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.514(d)(2)(ii) requires adequate separation between a group health plan and the Plan Sponsor. In addition, the classes of employees or other persons under the control of the Plan Sponsor to be given access to protected health information must be disclosed. Any access to protected health information provided to employees of the Plan Sponsor must be limited to the plan administration functions of the group health plans.

### **Policy**

It is the policy of OHCA Members to implement reasonable safeguards to limit access of workforce members to the information necessary to carry out their duties in relation to the group health plans maintained by the Plan Sponsor.

### **Procedures**

The following classes of personnel require and will maintain the indicated levels of access to protected health information to appropriately accomplish their duties and responsibilities:

- (a) Job Function: Health Benefits of the Human Resources Department Personnel
  - (i) Permitted Access to Protected Health Information: Health Benefits personnel of the Employer, including the Privacy Officer, shall have complete access to all health plan records. Health Benefits personnel must have full access to protected health information under the group health plans for proper administration of such plans. Health Benefits personnel may use or disclose protected health information for any reason permitted by this manual or by the HIPAA privacy rules.
  - (ii) Restrictions: None.
- (b) Job Function: Legal Department Personnel
  - (i) Permitted Access to Protected Health Information: Legal Department personnel of the Employer shall have limited access to protected health information. Legal Department personnel shall be permitted to access protected health information for purposes of litigation (including the anticipation of litigation) and for purposes of any claims dispute (or potential claims dispute) for the covered group health plans.
  - (ii) Restrictions: Legal Department personnel shall not use protected health information relating to the covered group health plans except as required or necessary to assist the Health Benefits with litigation (including the anticipation of litigation) and any claims dispute (or potential claims

dispute) for the covered group health plans. Legal Department personnel shall not disclose any protected health information relating to the covered group health plans except as required or necessary to assist Health Benefits with litigation (including the anticipation of litigation) and any claims dispute (or potential claims dispute) for the covered group health plans. Legal Department personnel shall at all times maintain the confidentiality of the protected health information that may be accessed in performing their duties.

- (c) Job Function: Accounting Division of the Finance Department Personnel
- (i) Permitted Access to Protected Health Information: Accounting Division of the Finance Department personnel of the Employer shall have limited access to protected health information. Accounting Division personnel shall be permitted to access protected health information when conducting an audit of the Health Benefits office or the operation of the covered group health plans.
  - (ii) Restrictions: Accounting Division personnel shall not use protected health information relating to the covered group health plans except as required to perform an audit of the Health Benefits office or the covered group health plans. Accounting Division personnel shall not disclose any protected health information relating to the covered group health plans to anyone other than the Privacy Officer and other Health Benefits personnel. Accounting Division personnel shall at all times maintain the confidentiality of the protected health information that may be accessed in performing their duties.
- (d) Job Function: Senior Management Assistant of the Human Resources Department
- (j) Permitted Access to Protected Health Information: The Senior Management Assistant of the Human Resources Department of the Employer shall have limited access to protected health information. The Senior Management Assistant shall be permitted to access protected health information when conducting cost utilization analysis with respect to the covered group health plans.
  - (ii) Restrictions: The Senior Management Assistant shall not use protected health information relating to the covered group health plans except as required to conduct cost utilization analysis with respect to the covered group health plans. The Senior Management Assistant shall not disclose any protected health information relating to the covered group health plans to anyone other than the Privacy Officer and other Health Benefits personnel. The Senior Management Assistant shall at all times maintain the confidentiality of the protected health information that may be accessed in performing their duties.



- (e) Job Function: Municipal Information Systems Department Personnel
- (i) Permitted Access to Protected Health Information: Municipal Information Systems ("MIS") Department personnel of the Employer shall have limited access to protected health information. MIS Department personnel shall be permitted to access protected health information when monitoring employee e-mails or backing-up the computer system of the Employer. Such MIS personnel shall also be permitted to assist OHCA Member personnel in case of a computer malfunction or other computer-related problem even if protected health information may be contained on the screen of a computer. The authorized personnel within the MIS Department may also have access to protected health information when installing new or updated software onto the computer network maintained by the Employer.
  - (ii) Restrictions: MIS Department personnel shall not use protected health information and shall not disclose protected health information. MIS Department personnel shall at all times maintain the confidentiality of the protected health information that may be accessed in performing their duties of ensuring proper operation of the Employer's computer network.
- (f) Job Function: City Manager
- (i) Permitted Access to Protected Health Information: The City Manager of the City of Corpus Christi shall have limited access to protected health information. The City Manager shall be permitted to access protected health information for purposes of litigation (including the anticipation of litigation) and for purposes of any claims dispute (or potential claims dispute) for the covered group health plans.
  - (ii) Restrictions: The City Manager shall not use protected health information relating to the covered group health plans except as required or necessary to assist Health Benefits with litigation (including the anticipation of litigation) and any claims dispute (or potential claims dispute) for the covered group health plans. The City Manager shall not disclose any protected health information relating to the covered group health plans except as required or necessary to assist Health Benefits with litigation (including the anticipation of litigation) and any claims dispute (or potential claims dispute) for the covered group health plans. The City Manager shall at all times maintain the confidentiality of the protected health information that may be accessed in performing their duties.

## **IV. IDENTIFYING WHEN ROUTINE HEALTH INFORMATION BECOMES PHI**

### **A. Determination of PHI Status**

**Effective: April 14, 2003**

#### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. To support this commitment, OHCA Members will ensure that the appropriate steps are taken to properly identify and secure individuals' protected health information, as required under 45 CFR Part 164, and other applicable federal, state, and/or local laws and regulations.

#### **Policy**

1. The following information will be designated as protected health information: Any health information, including demographic information collected from an individual, transmitted or maintained in any form or medium, that:
  - (a) is created or received by a health care provider, health plan, or health care clearinghouse; and
  - (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - (1) That identifies the individual; or
    - (2) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
2. Routine health information meeting the above definition will be automatically designated as protected health information immediately upon its creation or receipt by OHCA Members.
3. OHCA Members will adhere to all applicable laws, regulations, policies, and procedures when maintaining, using, and disclosing protected health information.

#### **Procedures**

1. The following persons, respectively, will be responsible for designating routine health information as protected health information.
  - (a) The Privacy Officer;
  - (b) The Assistant Privacy Officer;

- (c) The members of the Health Benefits office of the Employer;
- (d) The members of the Legal Department of the Employer;
- (e) The members of the Accounting Division of the Finance Department of the Employer;
- (f) The members of the MIS Department of the Employer;
- (g) The Senior Management Assistant of the Human Resources Department of the Employer; and
- (h) The Director of Human Resources, the Assistant City Manager and the City Manager of the City of Corpus Christi.

## **B. Creating De-Identified Information**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. Federal law allows certain entities to use or disclose protected health information for the purpose of creating de-identified information - that is, information that has been stripped of any elements that may identify the individual, such as name, birth date, or social security number. OHCA Members may, from time to time, use de-identified data for various purposes such as utilization review. In doing so, we will ensure that the appropriate administrative and technical processes are in place to properly de-identify protected health information, as well as to secure any methods of re-identification, as required under 45 CFR §164.514(a) and other applicable federal, state, and/or local laws and regulations.

### **Policy**

1. OHCA Members may create de-identified information for the following purposes:
  - (a) Plan utilization;
  - (b) Premium bids; and
  - (c) Any other legitimate purpose necessary for the proper administration of the group health plans, as determined by the Privacy Officer.
2. OHCA Members will not use or disclose the code or other means of record identification or mechanism used to re-identify health information for any other purpose than what is specifically required for the Plan Sponsor's internal operations.
3. De-identified information will not be disclosed if those OHCA Members and authorized employees of the Plan Sponsor creating or disclosing the information, or any other OHCA Members and the authorized employees of the Plan Sponsor, have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

### **Procedures**

1. The Privacy Officer will make decisions as to whether protected health information should be de-identified.
2. The reason for de-identification will be documented and maintained.
3. The following individually identifying elements will be removed or otherwise concealed from protected health information in order to create de-identified information:
  - (a) Names;

- (b) All elements of dates (except year) for dates directly related to an individual, including:
- birth date
  - admission date
  - discharge date
  - date of death
  - 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;
- (c) Telephone numbers;
- (d) Fax numbers;
- (e) Electronic mail addresses;
- (f) Social security numbers;
- (g) Medical record numbers;
- (h) Health plan beneficiary numbers,
- (i) Account numbers;
- (j) Certificate/license numbers;
- (k) Vehicle identifiers and serial numbers, including license plate numbers;
- (l) Device identifiers and serial numbers;
- (m) Web Universal Resource Locators (URLs);
- (n) Internet Protocol (IP) address numbers;
- (o) Biometric identifiers, including finger and voice prints;
- (p) Full face photographic images and any comparable images;
- (q) All geographic subdivisions smaller than a State, including
- street address
  - city
  - county
  - precinct
  - zip code, and their equivalent geocodes

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: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

- (r) Any other unique identifying number, characteristic, or code
- 4. The safe harbor method shall be utilized by the OHCA Members in de-identifying information. The authorized employees of the Plan Sponsor shall remove all identifiers set forth in Procedure 3 to de-identify protected health information.
- 5. The code or other means of record identification used to re-identify information will not be derived from or related to information about the individual and should not otherwise be capable of being translated so as to identify the individual. OHCA Members shall not use or disclose the code or other means of record identification for any other purpose except for its own internal operations, and shall not disclose the mechanism for re-identification.
- 6. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **C. Limited Data Sets**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. Federal law allows certain entities to use or disclose protected health information for the purpose of creating a limited data set. A limited data set is information that excludes specified direct identifiers that may identify the individual for the purposes of (1) research, (2) public health, or (3) health care operations. This policy is designed to ensure that the appropriate administrative and technical processes are in place to correctly use limited data sets in accordance with 45 CFR 164.514(e).

### **Policy**

1. OHCA Members may create limited data sets only for the following purposes:
  - (a) Health care operations;
  - (b) Public health; and
  - (c) Research.
2. OHCA Members must enter into a data use agreement with the limited data set recipient prior to disclosing the information contained in the limited data set.

### **Procedures**

1. The Privacy Officer will make decisions as to whether a limited data set is required to be used for health care operations, public health or research purposes.
2. The reason for creation of the limited data set will be documented and maintained.
3. The following direct identifiers of the individual or of relatives, employers, or household members of the individual shall be removed:
  - (a) Names;
  - (b) Postal address information, other than town or city, state and zip code;
  - (c) Telephone numbers;
  - (d) Fax numbers;
  - (e) Electronic mail addresses;
  - (f) Social security numbers;

- (g) Medical record numbers;
  - (h) Health plan beneficiary numbers;
  - (i) Account numbers;
  - (j) Certificate/license numbers;
  - (k) Vehicle identifiers and serial numbers, including license plate numbers;
  - (l) Device identifiers and serial numbers;
  - (m) Web Universal Resource Locators (URLs);
  - (n) Internet Protocol (IP) address numbers;
  - (o) Biometric identifiers, including finger and voice prints; and
  - (p) Full face photographic images and any comparable images.
4. OHCA Members may use protected health information to create a limited data set, or disclose protected health information to a business associate for such purpose, whether or not the limited data set is to be used by OHCA Members.
  5. OHCA Members may use or disclose a limited data set only if OHCA Members obtain satisfactory assurance, in the form of a data use agreement, that the limited data set recipient will only use or disclose the protected health information for limited purposes.
  6. The data use agreement between OHCA Members and the limited data set recipient must:
    - (a) Establish the permitted uses and disclosures of such information by the limited data set recipient. 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 privacy rules;
    - (b) Establish who is permitted to use or receive the limited data set; and
    - (c) 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 other than as provided for by the data use agreement;
      - report to OHCA Members any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
      - ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees 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.
7. If OHCA Members learn of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, OHCA Members must take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, OHCA Members must (1) discontinue disclosure of protected health information to the recipient and (2) report the problem to Health and Human Services.

## **V. TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS**

### **A. Disclosure of PHI for Treatment, Payment, and Health Care Operations**

**Effective: April 14, 2003**

Under the HIPAA privacy standards, each self-insured group health plan maintained by the Plan Sponsor (as set forth in the Policy entitled "General Guidelines") may use or disclose protected health information for treatment, payment, or health care operations without authorization from an individual under the following circumstances:

1. for the treatment, payment, or health care operation (TPO) functions of each of the self-insured group health plans (as set forth in the Policy entitled "General Guidelines");
2. for treatment activities of a health care provider;
3. for the payment activities of another covered entity or health care provider, as long as the recipient of the protected health information is that covered entity or health care provider;
4. for purposes of health care operations of the OHCA Members; and
5. to another covered entity that is not in the disclosing covered entity's OHCA, for the other covered entity's health care operations, subject to very specific conditions.

The terms treatment, payment, and health care operations, as well as health care provider and covered entity have specific meanings that must be understood before disclosure. See policies and procedures set forth in this ARTICLE V relating specifically to treatment, payment and health care operations.

For (5) above, the entities disclosing and receiving the information must have or have had a relationship with the individual and the purpose for the disclosure must pertain to that relationship and the disclosure is (i) for the purpose of health care fraud and abuse detection or compliance, (ii) to review the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance and to conduct training programs, accreditation, certification, licensing and credentialing activities or (iii) to conduct quality assessment and improvement activities such as case management and population-based activities as set forth in 45 CFR 164.501 under "health care operations."

Therefore, in light of the HIPAA privacy standards, the OHCA Members and the authorized employees of the Plan Sponsor may use and disclose the following types of health care information without the individual's permission, including but not limited to:

- Information required for the processing of claims;
- Information required for procuring stop-loss insurance;
- Information relating to case management programs;
- Information relating to disease management programs;

- Information relating to appeals;
- Information relating to resolving internal grievances;
- Information relating to the monitoring of provider performance;
- Information relating to the eligibility, enrollment or disenrollment of an employee from a group health plan; and
- Information relating to plan utilization.

If you have any questions regarding the permissibility of the disclosure or use of the information, please contact the Privacy Officer or the Assistant Privacy Officers.

## **B. Disclosure of PHI for Treatment Purposes**

**Effective: April 14, 2003**

### **Purpose**

Under the HIPAA privacy standards, OHCA Members may disclose protected health information for payment purposes without authorization from an individual. Treatment is defined as 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.

### **Policy**

1. OHCA Members will comply with the requirements set forth in 45 CFR §164.506(c) to use or disclose protected health information for treatment purposes.
2. OHCA Members will only disclose information for treatment purposes for its own treatment activities or the treatment activities of a health care provider.

### **Procedure**

1. When OHCA Members receive a request from a health care provider for treatment purposes, OHCA Members may provide information to such provider. The disclosure of such information is not subject to the minimum necessary standard.
2. Before disclosing the requested information to the health care provider, Privacy Officer, Assistant Privacy Officer or other authorized employees must verify the identity of the person making the request. See Policy entitled "Verification of Individuals or Entities Requesting Use or Disclosure of PHI."
3. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **C. Disclosure of PHI for Payment Purposes**

**Effective: April 14, 2003**

### **Purpose**

Under the HIPAA privacy standards, OHCA Members may disclose protected health information for treatment purposes without authorization from an individual. Payment is defined as the activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibilities for coverage and provision of benefits under the health plan or (ii) a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

### **Policy**

1. OHCA Members will comply with the requirements set forth in 45 CFR §164.506(c) to use or disclose protected health information for payment purposes.
2. OHCA Members will only use or disclose information for payment purposes for its own payment activities or the payment activities of another covered entity or a health care provider.

### **Procedure**

1. The uses and disclosures of protected health information for payment activities include, but are not limited to:
  - determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;
  - risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - 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;
  - review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and
  - disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (i) name and address, (ii) date of birth, (iii) social security number, (iv) payment history, (v) account number; and (vi) name and address of the health care provider and/or health plan.
2. Any use or disclosure of protected health information for payment activities is limited to the minimum necessary standard [See Policy entitled "Disclosing and Requesting only the Minimum Amount of PHI Necessary"] unless the information is required to be transmitted as an electronic transaction, pursuant to 45 CFR 160.102 and 45 CFR 164.502(b)(2)(vi).

3. Before disclosing the requested information to the covered entity or health care provider, Privacy Officer, Assistant Privacy Officer or other authorized employees must verify the identity of the person making the request. See Policy entitled "Verification of Individuals or Entities Requesting Use or Disclosure of PHI."
4. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **D. Disclosure of PHI for Health Care Operations**

**Effective: April 14, 2003**

### **Purpose**

Under the HIPAA privacy standards, OHCA Members may disclose protected health information for health care operation purposes without authorization from an individual. Health care operations include functions which allow a covered entity to carry out its treatment and payment activities and other functions covered under the privacy rule.

### **Policy**

1. OHCA Members will comply with the requirements set forth in 45 CFR §164.506(c) to use or disclose protected health information for health care operations purposes.
2. The self-insured health plans maintained by the Plan Sponsor that are OHCA Members may use or disclose information for health care operation purposes for their own health care operations.
3. OHCA Members may disclose protected health information about an individual to another covered entity that participates in the OHCA for any health care operation activities of the OHCA.
4. OHCA Members may disclose protected health information to another covered entity (which is not an OHCA Member) for health care operations activities of the entity that receives the information, only if (1) each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, (2) the protected health information pertains to such relationship and (3) the disclosure is (i) for the purpose of health care fraud and abuse detection or compliance, (ii) to review the competence or qualifications of health care professionals, evaluate practitioner and provider performance, health plan performance or to conduct training programs, accreditation, certification, licensing and credentialing activities or (iii) to conduct quality assessment and improvement activities such as case management and population-based activities as set forth in 45 CFR 164.501 under "health care operations."

### **Procedure**

1. The uses and disclosures of protected health information for health care operation activities may include, but are not limited to:
  - Conducting quality assessment and improvement activities including outcomes evaluation; 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;
  - Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance,

- conducting training programs, accreditation, certification, licensing, or credentialing activities;
- Underwriting, 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);
  - Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity;
  - Business management and general administrative activities of the entity, including but not limited to
    - Management activities relating to implementation of and compliance with the requirements of this subchapter;
    - Customer service;
    - Resolution of internal grievances;
    - The sale, transfer, merger or consolidation of all or part of the 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
    - The creation of de-identified health information or a limited data set.
2. Any use of disclosure of protected health information for health care operation activities is limited to the minimum necessary standard [See Policy entitled "Disclosing and Requesting only the Minimum Amount of PHI Necessary"].
  3. Before disclosing the requested information to another covered entity that is not an OHCA Member, Privacy Officer, Assistant Privacy Officer or other authorized employees must verify the identity of the person making the request [See Policy entitled "Verification of Individuals or Entities Requesting Use or Disclosure of PHI"].
  4. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.



## **E. Incidental Disclosures of PHI**

**Effective: April 14, 2003**

### **Purpose**

The HIPAA privacy standards permit certain incidental uses or disclosures of protected health information that occur as a by-product of another permissible use or disclosure of protected health information as long as reasonable safeguards and the minimum necessary standard have been utilized in relation to the primary use or disclosure of protected health information. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a result of another use or disclosure of protected health information permitted under the HIPAA privacy rules.

### **Policy**

1. OHCA Members will comply with the requirements set forth in the Policy entitled "Safeguards for Protected Health Information."
2. OHCA Members will comply with the requirements set forth in the Policy entitled "Disclosing and Requesting Only the Minimum Amount of PHI Necessary."
3. Incidental disclosures which cannot otherwise be prevented are allowable as long as OHCA Members and the authorized employees of the Plan Sponsor use reasonable safeguards to minimize the risk to an individual's privacy and follow the minimum necessary standard when using or disclosing such information.

### **Procedure**

1. OHCA Members and the authorized employees of the Plan Sponsor may make incidental disclosures which cannot otherwise be prevented as long as reasonable safeguards are used to minimize the risk to an individual's privacy and the minimum necessary standard is followed when using or disclosing such information.
2. Employees shall use reasonable precautions such as using lowered voices and talking apart from others when using or disclosing protected health information. For example, a health plan employee may discuss a claim on the telephone, even if such conversation is overheard by another employee not authorized to handle health plan information reasonable precautions are used and the minimum necessary amount of information is disclosed. Employees shall also clear all work areas of documents containing protected health information when not physically present at such work areas. Reasonable precautions shall be determined on a facts and circumstances basis based on the employee's professional judgment.
3. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **F. Treatment of Protected Health Information After Death**

**Effective: April 14, 2003**

### **Purpose**

HIPAA requires that protected health information of a deceased individual will be handled according to the policies and procedures applied to the protected health information of living individuals. The death of an individual does not reduce the privacy protections that such individual's protected health information will receive.

### **Policy**

OHCA Members will treat the protected health information of a deceased individual the same as the protected health information of living individuals, as set forth in this manual.

### **Procedure**

OHCA Members shall continue to apply all standards for the use and disclosure of protected health information as set forth in this manual to records of an individual who is deceased. Such treatment shall continue for the length of time OHCA Members maintain records on such individual.

## **VI. THE MINIMUM NECESSARY STANDARD**

### **A. Disclosing and Requesting Only the Minimum Amount of PHI Necessary**

**Effective: April 14, 2003**

#### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. While protected health information must be available to Health Benefits personnel in the process of performing required duties in relation to the operation of the health plans, we should avoid disclosing more protected health information than needed to perform our respective duties. To support our commitment to confidentiality, OHCA Members will ensure that the appropriate steps are taken to disclose only the minimum amount of protected health information necessary to accomplish the particular use or disclosure, as required under 45 CFR. 6164.502(b), and other applicable federal, state, and/or local laws and regulations.

#### **Policy**

1. OHCA Members and authorized employees of the Plan Sponsor will follow proper procedures to ensure that only the minimum amount of protected health information necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.
2. OHCA Members and authorized employees of the Plan Sponsor will request only the minimum amount of protected health information necessary to accomplish the specific purpose of the request.
3. This policy does not apply to the following uses or disclosures:
  - (a) disclosure to or requests by a provider for treatment;
  - (b) uses or disclosure made to the individual who is the subject of the information;
  - (c) uses or disclosure pursuant to an authorization;
  - (d) disclosure made to the Department of Health and Human Services;
  - (e) uses or disclosures required by law; and
  - (f) uses or disclosure required for compliance with applicable laws and regulations.

#### **Procedures**

1. All proposed uses or disclosures of protected health information will be reviewed by persons having an understanding of OHCA Members' privacy policies and practices, and sufficient expertise to understand and weigh the necessary factors.

2. OHCA Members will only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.
3. The following classes of personnel require and will maintain the indicated levels of access to protected health information to appropriately accomplish their duties and responsibilities:
  - (a) Job Function: Health Benefits office of the Human Resources Department Personnel
    - Permitted Access to Protected Health Information: Health Benefits personnel of the Employer, including the Privacy Officer, shall have complete access to all health plan records. Health Benefits personnel must have full access to protected health information under the group health plans for proper administration of such plans. Health Benefits personnel may use or disclose protected health information for any reason permitted by this manual or by the HIPAA privacy rules.
  - (b) Job Function: Legal Department Personnel
    - Permitted Access to Protected Health Information: Legal Department personnel of the Employer shall have limited access to protected health information. Legal Department personnel shall be permitted to access protected health information for purposes of litigation (including the anticipation of litigation) and for purposes of any claims dispute (or potential claims dispute) for the covered group health plans.
  - (c) Job Function: Finance Department Personnel
    - Permitted Access to Protected Health Information: Finance Department personnel of the Employer shall have limited access to protected health information. Finance Department personnel shall be permitted to access protected health information when conducting an audit of the Health Benefits office or the operation of the covered group health plans.
  - (d) Job Function: MIS Department Personnel
    - Permitted Access to Protected Health Information: MIS Department personnel of the Employer shall have limited access to protected health information. MIS Department personnel shall be permitted to access protected health information when monitoring employee e-mails or backing-up the computer system of the Employer. Such MIS personnel shall also be permitted to assist OHCA Member personnel in case of a computer malfunction or other computer-related problem even if protected health information may be contained on the screen of a computer. The authorized personnel within the MIS Department may also have access to protected

health information when installing new or updated software onto the computer network maintained by the Employer.

- (e) Job Function: Senior Management Assistant of the Human Resources Department
- Permitted Access to Protected Health Information: The Senior Management Assistant of the Human Resources Department of the Employer shall have limited access to protected health information. The Senior Management Assistant shall be permitted to access protected health information when conducting cost utilization analysis with respect to the covered group health plans.
- (f) Job Function: City Manager
- Permitted Access to Protected Health Information: The City Manager of the City of Corpus Christi shall have limited access to protected health information. The City Manager shall be permitted to access protected health information for purposes of litigation (including the anticipation of litigation) and for purposes of any claims dispute (or potential claims dispute) for the covered group health plans.
4. Access to protected health information will be reasonably limited to that described in Procedure 3 by reference to the Policy entitled "Allocation of Job Tasks for PHI-Related Functions."
5. The following criteria will be used in limiting the amount of protected health information requested, used, or disclosed by authorized personnel:
- (a) Does the requesting individual have complete understanding of the purpose for the request, use, or disclosure of the protected health information?
  - (b) Is the amount of information requested the minimum necessary to accomplish the purpose of the use or disclosure?
6. Requests for disclosures of protected health information will be reviewed on an individual basis in accordance with criteria listed in the policy.
7. Authorized personnel may reasonably rely on requests by:
- (a) public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;
  - (b) other covered entities in determining the minimum necessary information for certain disclosures; or
  - (c) by an individual who is a member of its workforce authorized to receive protected health information or is a business associate of OHCA Members for the purpose

of providing professional services to OHCA Members, if the professional represents that the information requested is the minimum necessary for the stated purpose.

8. In the event of disclosures for research purposes, OHCA Members will review the documentation of required Institutional Review Board or other approval in determining the minimum amount of protected health information necessary.
9. For any type of use or disclosure of protected health information made on a routine and recurring basis, OHCA Members shall only use or disclose the amount of information reasonably necessary to achieve the purpose of the task or to comply with the disclosure request. OHCA Members may rely on past practices in determining the amount of information needed to perform the particular function and will not be required to review on a case-by-case basis whether the information used or disclosed conforms to the minimum necessary standard.
10. For any type of use or disclosure of protected health information not made on a routine and recurring basis, OHCA Members shall only use or disclose the amount of information reasonably necessary to achieve the purpose of the task or to comply with the disclosure request, as is prudent under the particular circumstances. OHCA Members shall be required to review on a case-by-case basis whether the information used or disclosed conforms to the minimum necessary standard.
11. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **VII. DISCLOSURES TO PERSONS WITH A RELATIONSHIP TO AN INDIVIDUAL**

### **A. Personal Representatives**

**Effective: April 14, 2003**

#### **Purpose**

OHCA Members will sometimes need to use or disclose protected health information to a person who has legal authority to act on behalf of an individual. A covered entity, pursuant to 45 CFR 164.502(g) must treat a personal representative as the individual for purposes of HIPAA's privacy rules. A personal representative is defined as a person who legally has authority to make health care decisions on behalf of an individual. A personal representative may act on behalf of the individual for the purposes of authorizing the use and disclosure of protected health information, receiving information that otherwise would be sent to the individual and exercising individual rights provided under the HIPAA privacy rules.

#### **Policy**

1. If under applicable law, a parent, guardian or other person acting in loco parentis has the authority to act on behalf of an individual who is an unemancipated minor, OHCA Members must treat such person as a personal representative with respect to protected health information relevant to such personal representation, subject to certain exceptions listed below.
2. If under applicable law, a person has the authority to act on behalf of an individual who is an adult or an emancipated minor, OHCA Members must treat such person as a personal representative with respect to protected health information relevant to such personal representation.
3. 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, OHCA Members must treat such person as a personal representative with respect to protected health information relevant to such personal representation.
4. OHCA Members may elect to not treat a person as the personal representative of an individual if OHCA Members have a reasonable belief that (i) the individual has been or may be subjected to domestic violence, abuse or neglect by such person or (ii) treating such person as the personal representative could endanger the individual and OHCA Members decide that it is not in the best interest of the individual to treat the person as the individual's personal representative.

#### **Procedures**

1. An individual may designate a personal representative in writing. Alternatively, a person who is identified as having a power of attorney or other legal authority to act on behalf of

the individual will be recognized as a personal representative. OHCA Members may request documentation from the purported personal representative setting forth the legal authority to act on behalf of the individual before recognizing such person as the personal representative of the individual.

2. A parent or legal guardian of an unemancipated minor will be recognized as the personal representative of a child, unless state or other law permits the minor to request that information not be shared with a parent guardian or other person acting in loco parentis. The Privacy Officer shall review any minor's request for confidentiality pertaining to the use or disclosure of protected health information that relates to a parent or guardian to determine whether the request complies with state and federal laws.
3. A personal representative may sign any form (such as an authorization) or exercise individual rights (such as requesting an accounting of disclosures) on behalf of the individual. The personal representative will be treated as the individual with respect to all the rules governing uses and disclosures set forth in this manual.
4. A personal representative may receive protected health information concerning the individual necessary to carry out the representative's legal duties to the individual.
5. If a reasonable belief exists that (i) the individual has been or may be subjected to domestic violence, abuse or neglect by such person or (ii) treating such person as the personal representative could endanger the individual, such employee shall notify the Privacy Officer. The Privacy Officer shall be responsible for deciding that it is not in the best interest of the individual to treat the person as the individual's personal representative. Any requests from the purported personal representative concerning the individual should be referred to the Privacy Officer.



## **B. Using PHI for Involvement In and Notification of the Individual's Care**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members will sometimes need to use or disclose protected health information to an individual's family member or others involved in the individual's care. In these situations, when the individual is present and capacitated, OHCA Members must provide the individual with an opportunity to agree or disagree to the use or disclosure of such information, and if agreement is obtained, is not required to obtain the written authorization of the patient. Employees may orally inform the individual of and obtain the individual's oral agreement or objection to such uses or disclosures. OHCA Members may also obtain the individual's agreement to the use or disclosure to family members or close friends prior to the disclosure.

### **Policy**

1. OHCA Members may disclose to a family member, other relative, close personal friend, or any other person identified by the patient, protected health information that is directly relevant to such person's involvement with or payment related to the patient's care.
2. OHCA Members will follow all applicable laws and regulations when disclosing protected health information relevant to an individual's care to the patient's family member, friend, or any other person identified by the individual.

### **Procedures**

1. OHCA Members will seek agreement from each individual upon enrollment to disclose his or her protected health information relevant to the individual's care to the individual's identified family member, friend, or any other person identified by the individual.
2. If the individual is present and family members or close personal friends accompany such individual, OHCA Members may use or disclose protected health information in front of such family members or friends if:
  - (a) OHCA Members obtain the individual's agreement (which may be oral);
  - (b) OHCA Members provide the individual with the opportunity to object to the disclosure and the individual does not express an objection;
  - (c) OHCA Members have on file the names of the family members or close personal friends present to which the individual has provided OHCA Members upon enrollment pursuant to procedure 1 and such family members or friends are the persons accompanying the individual; or
  - (d) OHCA Members reasonably infer from the circumstances, based upon the exercise of professional judgment, that the individual does not object to the disclosure.

3. If necessary given the condition of the individual or critical circumstances involved, OHCA Members may reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure of health information relevant to the patient's care to the patient's family member, friend, or any other person identified by the individual.
4. OHCA Members may use or disclose protected health information 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 the entity to notify, or assist in the notification of 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.
5. In the event that the individual is not present for, 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, OHCA Members 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 protected health information that is directly relevant to the person's involvement with the individual's health care.
6. If a family member or close friend calls the Health Benefits office to discuss an individual's medical condition or benefit issue, benefits personnel may instruct such family member or close friend to have the individual whose medical records are at issue call the Health Benefits office to approve the communication. The Health Benefits office may communicate with a family member or close friend identified on the form provided by an individual to the Health Benefits office under Procedure 1 as long as the Health Benefits office can reasonably verify the identity of the caller as being the person listed on such form (*e.g.*, requiring such caller to provide the individual's security number or mother's maiden name).
7. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **VIII. REQUIRED DISCLOSURES OF PHI UNDER HIPAA**

**Effective: April 14, 2003**

### **Purpose**

A covered entity is required to disclose protected health information to the extent that such use or disclosure is requested by Health and Human Services or requested by the individual whose protected health information is at issue. This policy is designed to give guidance and ensure compliance with all relevant laws and regulations when required to disclose protected health information under the privacy rules.

### **Policy**

If requested by Health and Human Services or if requested by the individual whose protected health information is at issue, OHCA Members must disclose such protected health information.

### **Procedures**

1. OHCA Members must disclose protected health information to Health and Human Services when requested to investigate or determine OHCA Members' compliance with HIPAA's privacy rules.
2. OHCA Members must disclose protected health information to an individual when requested under, and as required under 45 CFR 164.524 (See Policy entitled "Granting Access to Inspect and Obtain a Copy of PHI") or 45 CFR 164.528 (See Policy entitled "Accounting of Disclosures").
3. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **IX. PERMITTED DISCLOSURES UNDER HIPAA**

### **A. Disclosing PHI as Required by Law**

**Effective: April 14, 2003**

#### **Purpose**

A covered entity may use or disclose protected health information 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. This policy is designed to give guidance and ensure compliance with all relevant laws and regulations when using or disclosing protected health information as required by law.

#### **Policy**

1. If federal, state, and/or local law requires a use or disclosure of protected health information, OHCA Members may use or disclose protected health information to the extent that the use or disclosure complies with such law and is limited to the requirements of such law.
2. OHCA Members will refer to specific policies and procedures as set forth in this Section IX to determine whether or not OHCA Members must obtain consent, authorization, or give the individual the opportunity to agree or object to use or disclosure of protected health information.
3. In the event that two or more laws or regulations governing the same use or disclosure conflict, OHCA Members will comply with the more restrictive laws or regulations.

#### **Procedures**

1. OHCA Members may use or disclose protected health information to the extent that such use or disclosure is required by law including, but not limited to:
  - (a) For public health activities required by law [see "Policy for Disclosing Protected Health Information for Public Health Release"];
  - (b) For disclosures about victims of abuse, neglect, or domestic violence [see "Policy for Disclosing Protected Health Information about Victims of Abuse, Neglect, or Domestic Violence"];
  - (c) In order to comply with judicial release [see "Policy for Disclosing Protected Health Information for Judicial and Administrative Release"];
  - (d) To comply with law enforcement [see "Policy for Disclosing Protected Health Information for Law Enforcement Release"];

- (e) For disclosures relating to decedents [see "Policy for Disclosing PHI about Decedents"];
  - (f) For disclosures relating to cadaveric organ donations [see "Policy for Disclosing PHI for Cadaveric Organ, Eye or Tissue Donation"];
  - (g) For disclosures for research [see "Policy for Research Release"];
  - (h) For purposes of worker's compensation programs [see "Policy for Disclosing PHI for Worker's Compensation"];
  - (i) For health release [see "Policy for Disclosing Protected Health Information for Health Oversight Release"];
  - (j) To avert serious threat [see Policy for Disclosing Protected Health Information to Avert Serious Threat to Health and Safety];
  - (k) To comply with special government functions or requests [see Policy for Disclosing Protected Health Information for Specialized Government Functions].
2. When disclosing protected health information in accordance with procedure 1, OHCA Members will follow the policies and procedures relating to the applicable policy as set forth in this Section IX.
  3. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting Protected Health Information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
  4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
  7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
  8. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, Health Benefits personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.

9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **B. Disclosing PHI for Public Health Release**

**Effective: April 14, 2003**

### **Purpose**

According to 45 CFR §164.512(b), covered entities are permitted to disclose protected health information to public health authorities for a full range of public health activities carried out by federal, state, and local public health authorities. The actual authorities and terminology used for public health activities will vary under different jurisdictions. This policy is designed to provide guidance and to ensure full compliance with all applicable laws related to the use and disclosure of protected health information for public health release purposes.

### **Policy**

1. OHCA Members may disclose protected health information for public health activities and purposes to public health authorities, entities, and persons authorized by law to receive such information.

### **Procedures**

1. OHCA Members through authorized Health Benefits personnel of the Plan Sponsor may disclose protected health information to a public health authority that is authorized by law to collect or receive such information (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) for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to the reporting of:
  - (a) disease;
  - (b) injury,
  - (c) vital events such as birth or death; and
  - (d) the conduct of public health surveillance, public health investigations, and public health interventions.
2. OHCA Members may disclose protected health information to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
3. OHCA Members may disclose protected health information to a person subject to the jurisdiction of and required or directed to report such information to the Food and Drug Administration in order to:
  - (a) report adverse events (or similar reports with respect to food or dietary supplements); product defects or problems (including problems with the use or labeling of a product); biological product deviations;

- (b) track products;
  - (c) enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems);
  - (d) conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration.
4. OHCA Members may disclose protected health information to a person who may have been exposed to a communicable disease; or may otherwise be at risk of contracting or spreading a disease, if OHCA Members or a public health authority is authorized by law to notify such person in the conduct of a public health intervention or investigation.
5. OHCA Members may disclose protected health information to an employer about an individual who is a member of the employer's workforce if OHCA Members either provide health care to the individual at the request of the employer or is a member of the employer's workforce:
- (a) to conduct an evaluation relating to medical surveillance of the workplace; or
  - (b) to evaluate whether the individual has a work-related illness or injury;
  - (c) If the protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
  - (d) If the employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and
  - (e) OHCA Members provide written notice to the individual that protected health information 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 work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.
6. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting Protected Health Information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health Information"].



7. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
8. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
9. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
10. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
11. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
12. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **C. Disclosing PHI about Victims of Abuse, Neglect, or Domestic Violence**

**Effective: April 14, 2003**

### **Purpose**

Covered entities are required to exercise professional judgment in conjunction with applicable statutes and regulations when disclosing protected health information regarding an individual who is a possible victim of abuse, neglect, or domestic violence pursuant to 45 CFR 164.512(c). OHCA Members have developed this policy to ensure any use or disclosure of protected health information related to victims of abuse, neglect, or domestic violence is in compliance with all applicable laws and regulations.

### **Policy**

OHCA Members may disclose protected health information about an individual whom it 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 such reports.

### **Procedures**

1. OHCA Members may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence:
  - (a) to the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or
  - (b) if the individual agrees to the disclosure (communication between OHCA Members and individual, including agreement, may be oral); or
  - (c) to the extent the disclosure is expressly authorized by statute or regulation and:
    - (1) OHCA Members, in the exercise of professional judgment, believe the disclosure to be necessary to prevent serious harm to the individual or other potential victims; or
    - (2) if the individual is incapacitated and unable to agree to disclosing their protected health information, a law enforcement or public official authorized to receive the report must represent that the protected health information, for which disclosure is sought, is not intended to be used against the individual. The official must also represent that immediate enforcement activity is dependent upon the disclosure and would be adversely affected by waiting until the individual is able to agree to the disclosure.

2. If OHCA Members disclose protected health information about an individual, in accordance with Procedure 1, OHCA Members will promptly inform the individual, that such a disclosure has been or will be made except when OHCA Members:
  - (a) in the exercise of professional judgment, believes informing the individual would place him/her at risk of serious harm; or
  - (b) would be informing a personal representative, and OHCA Members reasonably believe the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by OHCA Members in the exercise of professional judgment.
3. OHCA Members will report child abuse or neglect without restriction to the public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
4. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
5. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
6. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
7. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
8. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
9. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
10. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **D. Disclosing PHI for Health Oversight Release**

**Effective: April 14, 2003**

### **Purpose**

A covered entity may use or disclose protected health information without individual authorization for health oversight activities pursuant to 45 CFR §164.512(d), OHCA Members are committed to ensuring the privacy of protected health information. To support this commitment, OHCA Members will ensure any use or disclosure of Protected Health Information for health oversight release is in compliance with all applicable laws and regulations. This policy is designed to provide guidance when using or disclosing Protected Health Information for health oversight activities, while protecting health information in our possession.

### **Policy**

1. OHCA Members may disclose protected health information 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; except as otherwise stated in this policy and procedure.
2. If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits unrelated to health, OHCA Members consider the joint activity or investigation to be a health oversight activity.
3. OHCA Members will not disclose protected health information without authorization in cases where an individual is the subject of the investigation or other activity; if such investigation or other activity does not arise out of and is not directly related to:
  - (a) the receipt of health care;
  - (b) a claim for public benefits related to health;
  - (c) qualification for or receipt of public benefits or services when an individual's health is integral to the claim for public benefits or services.

### **Procedures**

1. OHCA Members may disclose protected health information 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 the following:
  - (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.
2. OHCA Members may disclose protected health information without authorization to a health oversight agency if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health.
  3. OHCA Members will not disclose protected health information without authorization in cases where an individual is the subject of the investigation or other activity; if such investigation or other activity does not arise out of and is not directly related to:
    - (a) the receipt of health care;
    - (b) a claim for public benefits related to health;
    - (c) qualification for or receipt of public benefits or services when an individual's health is integral to the claim for public benefits or services.
  4. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
  5. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  6. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  7. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
  8. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
  9. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.

10. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **E. Disclosing PHI for Judicial and Administrative Release**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. For most disclosures other than the usual course of treatment, payment, or health care operations, we must obtain individual authorization before using or disclosing the individual's protected health information. However, protected health information may be disclosed pursuant to a judicial or administrative process without the written authorization of the individual, or the opportunity for the individual to agree or object, in the situations and subject to the applicable requirements of 45 CFR §164.512(e). To support our commitment to confidentiality, OHCA Members will ensure any use or disclosure of protected health information for judicial and/or administrative release is in compliance with all applicable laws and regulations. From time to time an order from a court or administrative tribunal may request protected health information. This policy has been developed to provide guidance and to ensure full compliance with such requests, while protecting health information in our possession.

### **Policy**

1. OHCA Members will comply with all lawful and appropriate requests from regulatory and judicial authorities and may disclose protected health information necessary to respond to:
  - (a) a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal (subject to certain restriction discussed below), or
  - (b) a subpoena, discovery request, or other lawful process that is accompanied by an order of a court or administrative tribunal.
2. Disclosures will be made of only that protected health information that is expressly authorized in an appropriate request.

### **Procedures**

1. OHCA Members may disclose protected health information in the course of any judicial or administrative proceeding in response to a court order or an order of an administrative tribunal provided that OHCA Members disclose only the protected health information expressly authorized by such order.
2. If OHCA Members receive a subpoena, discovery request or other lawful process that is not accompanied by a court order or an order of an administrative tribunal, OHCA Members will disclose protected health information only after obtaining satisfactory assurance from the requesting party that they have made reasonable efforts to provide notice to the individual who is the subject of the requested protected health information or to secure a qualified protective order. The following requirements will apply:

- (a) OHCA Members will obtain a written statement and accompanying documentation from the requesting party demonstrating that a notice has been given (or a good faith attempt to provide notice has been made) to the individual that contained sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal.
  - (b) Where reasonable efforts have been made to ensure that the individual has been given notice of the request, OHCA Members will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
    - (1) Time for raising objections to the court or administrative tribunal has elapsed, and
    - (2) No objections were filed, or
    - (3) The court has resolved all objections filed by the individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.
  - (c) Where reasonable efforts have been made to secure a qualified protective order, OHCA Members will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
    - (1) Parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or
    - (2) Party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
    - (3) A qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that 1) prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested and 2) requires the return to the covered entity or destruction of the protected health information (including all copies) at the end of the litigation or proceeding.
  - (d) OHCA Members may disclose protected health information in response to lawful process without receiving satisfactory assurances described above if OHCA Members makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of Procedure 2(a) and (b) or Procedure 2(c).
3. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health information"].



4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
8. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **F. Disclosing PHI for Law Enforcement Release**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. For most disclosures other than for treatment, payment, or health care operations, OHCA Members must obtain individual authorization before using or disclosing the individual's protected health information. However, pursuant to a law enforcement process, and subject to the applicable requirements of 45 CFR §164.512(f), protected health information may be disclosed without the written consent or authorization of the individual, or the opportunity for the individual to agree or object. To support our commitment to confidentiality, OHCA Members will ensure any use or disclosure of protected health information for law enforcement release is in compliance with all applicable laws and regulations. From time to time a law enforcement agency or court may request protected health information. This policy has been developed to provide guidance and to ensure full compliance with such requests, while protecting health information in OHCA Members' possession.

### **Policy**

OHCA Members may disclose protected health information for law enforcement purposes to a law enforcement official if all applicable conditions have been met.

### **Procedures**

1. OHCA Members may disclose protected health information as required by law including laws that require the reporting of certain types of wounds or other physical injuries (excluding reports of abuse, neglect, or domestic violence).
2. OHCA Members may disclose protected health information without individual authorization in compliance with and as limited by the relevant requirements of a court order, court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.
3. OHCA Members may disclose requested protected health information pursuant to an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, under the following conditions:
  - (a) OHCA Members determines, in conjunction with the requesting party, that the information sought is relevant and material to a legitimate law enforcement inquiry.
  - (b) OHCA Members determines, in conjunction with the requesting party, that the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

- (c) OHCA Members determines, in conjunction with the requesting party, that de-identified information could not reasonably be used.
4. OHCA Members may disclose the following protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that OHCA Members 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.
  5. Other than stated within this policy, OHCA Members will not disclose any protected health information related to an individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue 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.
  6. OHCA Members may disclose to a law enforcement official protected health information that OHCA Members believes in good faith constitutes evidence of criminal conduct that occurred on the premises of OHCA Members.
  7. OHCA Members may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if OHCA Members have a suspicion that such death may have resulted from criminal conduct.
  8. OHCA Members may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime if the individual agrees to the disclosure.
  9. In cases where the individual is suspected to be a victim of a crime and where OHCA Members are unable to obtain the individual's agreement because of incapacity of other emergency circumstance, it will:

- (a) obtain representation from the official that such information is needed to determine whether a violation of law by a person other than the victim occurred, and such information is not intended to be used against the victim;
  - (b) obtain representation from the law enforcement official 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
  - (c) in the exercise of professional judgment, make a determination that the disclosure is in the best interest of the individual before disclosing protected health information.
10. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see "Policy for Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
  11. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  12. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  13. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
  14. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
  15. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
  16. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **G. Disclosing PHI about Decedents**

**Effective: April 14, 2003**

### **Purpose**

Covered entities are permitted to disclose protected health information to coroners and medical examiners and to funeral directors, as necessary and consistent with applicable law. This policy is designed to give guidance and ensure compliance with applicable laws and regulations when disclosing protected health information to coroners, medical examiners, and funeral directors.

### **Policy**

1. OHCA Members may disclose protected health information to coroners, medical examiners, and funeral directors pursuant to applicable law.

### **Procedures**

1. OHCA Members may disclose protected health information about a deceased person, without individual authorization, to coroners, medical examiners, or funeral directors for the following purposes:
  - (a) Identifying a deceased person, determining a cause of death, or other duties as authorized by law.
  - (b) To assist funeral directors, in carrying out their duties with respect to the decedent including, if necessary, disclosing protected health information prior to, and in reasonable anticipation of, the individual's death.
2. If OHCA Members perform the duties of a coroner or medical examiner OHCA Members may use protected health information for the above purposes.
3. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see Policy entitled "Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
8. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **H. Disclosing PHI for Cadaveric Organ, Eye, or Tissue Donation**

**Effective: April 14, 2003**

### **Purpose**

A covered entity may use or disclose protected health information 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. This policy is designed to provide guidance and ensure compliance with applicable laws when disclosing protected health information for purposes of organ, eye, or tissue donation.

### **Policy**

1. OHCA Members may use or disclose protected health information 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.

### **Procedures**

1. OHCA Members may use or disclose protected health information 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.
2. OHCA Members may make a use or disclosure under this policy without obtaining consent, authorization, or giving the individual the opportunity to agree or object.
3. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting protected health information [see Policy entitled "Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.

8. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.



## **I. Disclosing PHI to Avert Serious Threat to Health and Safety**

**Effective: April 14, 2003**

### **Purpose**

Covered entities are permitted, consistent with applicable law and standards of ethical conduct, to disclose protected health information based on a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. This policy provides guidance to ensure full compliance with all laws when using or disclosing protected health information to prevent or lessen a threat to the health or safety of a person or the public.

### **Policy**

1. OHCA Members, consistent with all applicable laws, may use or disclose protected health information, if OHCA Members, 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.
2. OHCA Members may make disclosures to persons or entities that are reasonably able to prevent or lessen the threat, including to the target of the threat. Further, OHCA Members will make such disclosures only when the belief is based upon OHCA Members' actual knowledge, or in reliance on a credible representation by a person with apparent knowledge or authority.

### **Procedures**

1. Consistent with applicable law, standards of ethical conduct, and this policy, OHCA Members may use or disclose protected health information under the following circumstances:
  - (a) To prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
  - (b) For law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that OHCA Members reasonably believe may have caused serious physical harm to the victim;
  - (c) For law enforcement authorities to identify or apprehend an individual where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody;
2. The information disclosed to identify or apprehend an individual made pursuant to a statement by the individual admitting participation in a violent crime that OHCA Members reasonably believe may have caused serious physical harm to the victim shall

contain only that specific statement, and shall contain only the following protected health 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.
3. OHCA Members will not use or disclose protected health information for law enforcement authorities to identify or apprehend an individual because the individual makes a statement admitting participation in a violent crime that OHCA Members reasonably believe may have caused serious physical harm to the victim:
    - (a) If such admission in participation is learned by OHCA Members in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or
    - (b) If such admission in participation is learned by the covered entity through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy to affect the propensity to commit the criminal conduct that is the basis for the disclosure.
  4. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting Protected Health Information [see Policy entitled "Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
  5. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  6. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  7. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
  8. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.

9. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
10. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **J. Disclosing PHI for Specialized Government Functions**

**Effective: April 14, 2003**

### **Purpose**

Under certain circumstances, and if certain requirements are met, a covered entity may use and disclose the protected health information for specialized government functions. This policy has been developed to provide guidance and ensure compliance with all applicable laws and regulations when disclosing protected health information for specialized government functions.

### **Policy**

1. OHCA Members may use and disclose protected health information without individual authorization for the following specialized government functions: Military and veterans activities; National security and intelligence activities; Protective services for the President and others; Medical suitability determinations; Correctional institutions and other law enforcement custodial situations.
2. OHCA Members will comply with all requirements under 45 CFR §164.512(k) when using or disclosing protected health information for specialized government functions.

### **Procedures**

1. OHCA Members may disclose protected health information of individuals in the Armed Forces without individual authorization for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, given that the appropriate military command authorities and the purposes for which the protected health information may be used or disclosed must be published in the Federal Register.
2. OHCA Members may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 USC 401, et seq.) and implementing authority (e.g., Executive Order 12333), or; for the provision of protective services to the President or other persons authorized by 18 USC 3056, or, to foreign heads of state or other persons authorized by 22 USC 2709(a)(3), or for the conduct of investigations authorized by 18 USC 871 and 879.
3. OHCA Members may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under Procedure 1.
4. OHCA Members may disclose protected health information to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual, if the correctional institution or law enforcement official represents that such information is necessary for:

- (a) the provision of health care to such individuals;
  - (b) the health and safety of such individual or other inmates;
  - (c) the health and safety of the officers or employees of or others at the correctional institution;
  - (d) the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
  - (e) law enforcement on the premises of the correctional institution; and
  - (f) the administration and maintenance of the safety, security, and good order of the correctional institution.
5. An OHCA Member which is a health plan that is a government program providing public benefits, may disclose protected health information relating to eligibility for 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 required or expressly authorized by statute or regulation.
  6. An OHCA Member which is a government agency administering a government program providing public benefits, may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.
  7. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting Protected Health Information [see Policy entitled "Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
  8. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  9. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  10. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

11. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
12. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
13. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **K. Disclosing PHI for Worker's Compensation**

**Effective: April 14, 2003**

### **Purpose**

A covered entity may disclose protected health information as authorized by and 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. This policy was developed to provide guidance and ensure compliance with applicable laws when disclosing protected health information related to workers compensation and other similar programs.

### **Policy**

OHCA Members may disclose protected health information 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.

### **Procedures**

1. OHCA Members may disclose protected health information 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.
2. Any disclosure of protected health information not specifically required under applicable state law shall be subject to the minimum necessary standard [see Policy entitled "Disclosing and Requesting Only the Minimum Amount of PHI Necessary"]
3. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting Protected Health Information [see: Policy entitled "Verification of Entities Requesting Use or Disclosure of Protected Health Information"].
4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.

8. In the event that the identity and legal authority of an individual or entity requesting Protected Health Information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.



## **X. VERIFICATION OF INDIVIDUALS OR ENTITIES REQUESTING USE OR DISCLOSURE OF PHI**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members are committed to ensuring the privacy and security of protected health information. In the normal course of business and operations, we will receive many requests to disclose protected health information for various purposes. To support our commitment to confidentiality, OHCA Members will ensure that the appropriate steps are taken to verify the identity and authority of individuals and entities requesting protected health information, as required under 45 CFR §164.514(h) and other applicable federal, state, and/or local laws and regulations.

### **Policy**

OHCA Members will take necessary steps to verify the identity and legal authority of persons requesting disclosure of protected health information.

### **Procedures**

1. In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of protected health information, authorized personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing protected health information:
  - (a) documentation, statements, or representations (either oral or written) that, on their face, meet the applicable requirements for a disclosure of protected health information;
  - (b) presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person;
  - (c) a written statement on appropriate government letterhead that the person is acting under the government's authority;
  - (d) other evidence or documentation from an 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;
  - (e) a written statement of the legal authority under which the information is requested;
  - (f) if a written statement would be impracticable, an oral statement of such legal authority;

- (g) a request that is made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority.
2. Health Benefits personnel may rely on the exercise of professional judgment in making the following uses or disclosures of protected health information:
    - (a) a use or disclosure to others in the involvement in the individual's care, or
    - (b) acting on a good faith belief in making a disclosure to avert a serious threat to health and safety.
  3. Personnel will report any discrepancies in the verification of the identity and/or legal authority of an individual or entity requesting Protected Health Information to the Privacy Officer in a timely manner.
  4. The Privacy Officer shall make the determination as to whether the disclosure is appropriate under the HIPAA privacy rules and whether the information shall be disclosed.
  5. Once it is determined that use or disclosure is appropriate, the Privacy Officer, Assistant Privacy Officer or other authorized employees will access the individual's protected health information using proper access and authorization procedures.
  6. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
  7. The Privacy Officer, Assistant Privacy Officer or other authorized employees will appropriately document the request and delivery of the protected health information.
  8. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
  9. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **XI. AUTHORIZATIONS**

### **A. Authorization to Use or Disclose PHI**

**Effective: April 14, 2003**

#### **Purpose**

HIPAA requires a covered entity to obtain authorization to use or disclose protected health information for all purposes not explicitly permitted under the regulations. As such, OHCA Members have created the following policies and procedure to comply with all applicable laws and regulations in relation to obtaining authorizations from individuals for uses or disclosures of protected health information not specifically permitted under HIPAA.

#### **Policy**

1. OHCA Members will comply with the requirements set forth in 45 CFR §164.508, to request authorization to use or disclose protected health information.
2. Except as stated in the Policy entitled "Conditioning Services or Eligibility on the Provision of an Authorization to Disclose Protected Health Information", OHCA Members will not condition benefits on the provision of an authorization.

#### **Procedure**

1. The authorization will be written in plain language.
2. Any authorization for the disclosure of protected health information will contain the following:
  - (a) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
  - (b) a description of each purpose of the requested use or disclosure;
  - (c) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
  - (d) the name or other specific identification of the person(s), or class of persons, to whom OHCA Members may make the requested use or disclosure;
  - (e) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
  - (f) statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;
  - (g) a description of how the individual may revoke the authorization;

- (h) a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by 45 CFR Part 164;
  - (i) the signature of the individual; or signature of personal representative with a description of the personal representative's authority to act for the individual and documentation of verification of that identity; and date;
  - (j) a statement that the individual may refuse to sign the authorization;
  - (k) for marketing uses or disclosures, if applicable, a statement that the use or disclosure of the requested information will result in direct or indirect remuneration to OHCA Members from a third party;
  - (l) a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure, except as provided in the Policy entitled "Conditioning Services or Eligibility on the Provision of an Authorization to Disclose Protected Health Information."
3. In all other cases, benefits personnel may request any reasonable form of identification to verify the identity of an individual.
  4. In addition, as part of the authorization process, OHCA Members will provide individuals with any facts they need to make an informed decision as to whether to allow release of the information.
  5. OHCA Members will document and retain the signed authorization for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.
  6. OHCA Members will provide the individual with a copy of the signed authorization.
  7. The authorization will not be combined with another document to create a compound authorization, unless:
    - (a) the other document is a similar such authorization;
    - (b) the authorization is for the use or disclosure of protected health information created for research that includes treatment of the individual.

## **B. Conditioning Services or Eligibility on the Provision of an Authorization to Disclose PHI**

**Effective: April 14, 2003**

### **Purpose**

Generally, OHCA Members may not condition the provision of treatment, payment, enrollment, or eligibility for benefits on the provision of an authorization to use or disclose an individual's protected health information. However, certain exceptions apply. OHCA Members are committed to ensuring that all individuals receive the highest quality of benefits, and therefore will take necessary steps to comply with applicable laws and regulations regarding the conditioning of benefits on an authorization.

### **Policy**

1. OHCA Members may condition the following on the provision of an authorization requested by OHCA Members:
  - (a) enrollment in a self-insured group health plan or eligibility for benefits if the authorization is requested by OHCA Members prior to an individual's enrollment, and if the authorization is sought for such group health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations;
  - (b) payment of a claim for specified benefits if the disclosure is necessary to determine payment of such claim.
2. OHCA Members will not condition enrollment, eligibility, or payment of a claim on the provision of an authorization for the use or disclosure of psychotherapy notes.

### **Procedure**

1. All requests for disclosures of protected health information that require authorization will be directed to the Assistant Privacy Officer or the Privacy Officer.
2. The Assistant Privacy Officer or Privacy Officer, in close consultation with the requesting party, will determine the nature of the request, and whether it is necessary to condition payment or services on obtaining the authorization. The policies stated herein will be the deciding factors.
3. If such conditions are determined necessary, then the Assistant Privacy Officer or Privacy Officer will inform the enrollee, potential enrollee, or applicable provider, including the reason for the conditioning of services.

## **C. Individual Revocation of an Authorization to Disclose PHI**

**Effective: April 14, 2003**

### **Purpose**

As organizations request authorization from individuals to use their protected health information, there will be cases where individuals will initially grant authorization, only to change their mind later. In these instances, OHCA Members have created policies and procedures to accommodate individuals who may wish to revoke their authorization.

### **Policy**

1. OHCA Members will allow an individual to revoke an authorization to use or disclose their protected health information, except in situations where:
  - (a) OHCA Members have taken action in reliance thereon;
  - (b) the authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy.
2. OHCA Members will take all necessary steps to honor and comply with an individual revocation of an authorization to use or disclose protected health information, unless stated otherwise in this policy.

### **Procedure**

1. OHCA Members will not impose a time restriction on when an individual may revoke authorization to use or disclose their protected health information.
2. OHCA Members will require individuals to request the revocation of authorization to use or disclose protected health information in writing.
3. All written revocations of authorizations shall be documented in accordance with the Policy entitled "Maintaining Appropriate Documentation Regarding Compliance with HIPAA Privacy Regulations."

## **D. Prohibiting the Use of an Invalid Authorization to Disclose PHI**

**Effective: April 14, 2003**

### **Purpose**

When obtaining an authorization for the use or disclosure of protected health information, it is important that the document contain all necessary information. If not, the authorization is defective and therefore invalid. OHCA Members have created policies and procedures addressing how an authorization could be defective to assist in preventing invalid authorizations.

### **Policy**

1. OHCA Members prohibit the use of an invalid authorization to use or disclose protected health information.
2. An authorization will become invalid in the event that OHCA Members know that the authorization has been revoked.

### **Procedure**

1. OHCA Members will invalidate an authorization upon the following events:
  - (a) the expiration date has passed or the expiration event is known by OHCA Members to have occurred;
  - (b) all of the required elements of the authorization have not been filled out completely, as applicable;
  - (c) the authorization lacks any of the required elements specified in Policy entitled "Authorization to Disclose Protected Health Information" as required for the purpose of applicable use or disclosure;
  - (d) the authorization is inappropriately combined with any other document to create a compound authorization.
  - (e) If any material information in the authorization is known by OHCA Members to be false.

## **E. Authorization for the Use or Disclosure of Psychotherapy Notes**

**Effective: April 14, 2003**

### **Purpose**

In most cases, HIPAA requires that covered entities obtain individual authorization before using or disclosing psychotherapy notes. OHCA Members are committed to ensuring that it obtains valid authorization for its use or disclosure of protected health information, specifically psychotherapy notes. Psychotherapy notes mean any notes recorded (in any medium) by a health care provider who is a mental health professional. These notes could be documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

### **Policy**

1. OHCA Members will obtain an individual's authorization prior to use or disclosure of psychotherapy notes.
2. OHCA Members may use or disclose psychotherapy notes in the following instances without obtaining authorization:
  - (a) use or disclosure that is required by 45 CFR §164.502(a)(2)(ii) [compliance investigations];
  - (b) use or disclosure permitted by 45 CFR §164.512(a) [as required by law];
  - (c) use or disclosure permitted by 45 CFR §164.512(d) [health oversight] with respect to the oversight of the originator of the psychotherapy notes;
  - (d) use or disclosure permitted by 45 CFR §164.512(g)(1) [decedents];
  - (e) use or disclosure permitted by 45 CFR §164.512(j)(1)(i) [threat to public safety].

### **Procedure**

1. OHCA Members will not condition treatment of an individual on a requirement that the individual provide a specific authorization for the disclosure of psychotherapy notes.
2. The authorization will be written in plain language.
3. The authorization may only be combined with another authorization for a use or disclosure of psychotherapy notes.



4. Any authorization for the use or disclosure of psychotherapy notes will contain the following:
  - (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 of other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
  - (d) the signature of the individual and date;
  - (e) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
  - (f) a statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;
  - (g) a description of how the individual may revoke the authorization; and
  - (h) a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by 45 CFR Part 164.
5. In the event that the authorization is signed by a personal representative of the individual, the authorization will contain a description of the representative's authority to act for the individual.
6. OHCA Members will invalidate the authorization if:
  - (a) the expiration date has passed or the expiration event is known by OHCA Members to have occurred,
  - (b) any material information in the authorization is known by the covered entity to be false;
  - (c) the requirements of the authorization have not been filled out completely.
7. OHCA Members will document and retain the signed authorization for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

## **XII. NOTICE OF PRIVACY PRACTICES**

### **A. Content of Notice**

**Effective: April 14, 2003**

#### **Purpose**

45 CFR §164.520 requires that notice be given to individuals of the use and disclosure of protected health information as well as the individual's rights and a covered entity's legal duties with respect to protected health information. This policy is designed to give guidance and to ensure compliance with all laws and regulations regarding the content of the Notice of Privacy Practices.

#### **Policy**

1. OHCA Members will give adequate notice to individuals regarding the use or disclosure of their protected health information, their rights with respect to such use or disclosure, and OHCA Members' legal duties pursuant to 45 CFR §164.520.
2. The content of the notice regarding the use and disclosure of protected health information pursuant to 45 CFR §164.520 shall comply with the policies and procedures that are described herein.

#### **Procedures**

1. Notice given to an individual regarding the use and disclosure of protected health information must be written in plain language and contain the statement prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAYBE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
2. The notice must contain descriptions in sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by HIPAA and other applicable laws, including:
  - (a) A description and at least one example, of the types of uses and disclosures that OHCA Members are permitted by law to make for each of the following purposes: treatment, payment, and health care operations.
  - (b) A description of each of the other purposes for which OHCA Members are permitted or required by the Privacy regulations to use or disclose protected health information without the individual's written consent or authorization;
  - (c) Information which OHCA Members will disclose protected health information without the individual's written consent or authorization including:
    - uses and disclosures required by law

- uses and disclosures for public health activities
  - disclosures about victims of abuse, neglect or domestic violence
  - uses and disclosures for health oversight activities
  - disclosures for judicial and administrative proceedings
  - disclosures for law enforcement purposes
  - uses and disclosures about decedents
  - uses and disclosures for cadaveric organ, eye or tissue donation purposes
  - uses and disclosures for research purposes
  - uses and disclosures to avert a serious threat to health or safety
  - uses and disclosures for specialized government functions
  - disclosures for workers compensation
3. If a use or disclosure described in parts (a) and (b) of procedure 2 are prohibited or materially limited by other laws, the description of the disclosure must reflect the more stringent law.
4. The notice must also contain the following statements or information:
- (a) a statement indicating other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as permitted by the individual's rights under HIPAA;
  - (b) a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise those rights:
    - the right to request restrictions on certain uses and disclosures of protected health information;
    - a statement that OHCA Members are not required to agree to a requested restriction;
    - the individual's right to receive confidential communications of protected health information, as applicable;
    - a statement and a brief description of how the individual may exercise his/her right to inspect, copy, amend, and receive an accounting of disclosures of protected health information;
    - a statement and a brief description of how the individual may exercise his/her right to obtain a paper copy of the notice from the covered entity, even if the individual has agreed to receive the notice electronically;
  - (c) a statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;
  - (d) a statement that the covered entity is required to abide by the terms of the notice that is currently in effect;
  - (e) a statement indicating that, for protected health information that it created or received prior to issuing a revised notice, OHCA Members reserve the right to

change the terms of its notice and to make the new notice provisions effective for all protected health information that they maintain;

- (f) a statement that OHCA Members will promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice, and how it will provide individuals with the revised notice;
  - (g) a statement that individuals may complain to OHCA Members and to the Department of Health and Human Services if they believe their privacy rights have been violated;
  - (h) a brief description of how an individual may file a complaint with OHCA Members;
  - (i) a statement that the individual will not be retaliated against for filing a complaint;
  - (j) the name, or title, and telephone number of a person or office within OHCA Members to contact for further information concerning the notice of privacy practices;
  - (k) the date on which the notice is first in effect, which is not to be earlier than the date on which the notice is printed or otherwise published.
5. If applicable, the description in the notice of the types of uses and disclosures that the OHCA Members are permitted to make for purposes of treatment, payment, and health care operations (see procedure 2(a)) must also include separate statement indicating that:
- A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the Plan Sponsor of the plan.
6. If OHCA Members choose to apply and describe more limited uses or disclosure in its notice than required under 45 CFR Part 164, then it will ensure that it does not include in the notice a limitation affecting its right to make a use or disclosure that is required by law or permitted to avert a serious threat to health and safety.
7. OHCA Members will promptly revise and redistribute their notice whenever there is a material change to the uses or disclosures, the individual's rights, OHCA Members' legal duties, or other privacy practices stated in the notice.
8. OHCA Members will not implement a material change to any term of the notice prior to the effective date of the notice in which such material change is reflected, except when required by law.
9. Upon making a change to a notice and policies and procedures due to a change in law, OHCA Members may use the notice revision date as the new effective date.

10. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the compliance hotline.

## **B. Provision of Notice of Privacy Practices**

**Effective: April 14, 2003**

### **Purpose**

45 CFR §164.520 requires that notice be given to individuals of the use and disclosure of protected health information as well as the individual's rights and a covered entity's legal duties with respect to protected health information. This policy is designed to provide guidance and to ensure compliance with all laws and regulations regarding the provision of the notice of use of protected health information by health plans.

### **Policy**

1. OHCA Members will provide a formal notice to individuals regarding the use or disclosure of protected health information pursuant to 45 CFR §164.520.
2. The provision of the notice given to individuals regarding the use and disclosure of protected health information pursuant to 45 CFR §164.520 will comply with the policies and procedures described herein.

### **Procedures:**

1. The notice will be provided as follows:
  - (a) no later than the compliance date for OHCA Members, to individuals then covered under the applicable group health plans, and thereafter, at the time of enrollment, to individuals who are new enrollees;
  - (b) within 60 days of a material revision to the notice, to individuals then covered by the applicable group health plans;
  - (c) no less frequently than once every three years to individuals then covered by the applicable group health plans of the availability of the notice and how to obtain the notice;
  - (d) to the named insured of a policy under which coverage is provided or to the named insured and one or more dependents.
2. If more than one notice exists, OHCA Members will provide the notice that is relevant to the individual or other person requesting the notice.
3. OHCA Members will only use a joint notice when all other covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by OHCA Members as part of their participation in the organized health care arrangement.
4. All joint notices will:

- (a) contain all of the specifications required of a single-entity notice and describe with reasonable specificity the covered entities, or class of entities, and service delivery sites, or classes of service delivery sites, to which the joint notice applies;
  - (b) contain all of the specifications required of a single-entity notice and, if applicable, state that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement;
  - (c) be provided to individuals within the same requirements as a single-entity notice.
5. OHCA Members will prominently post its notice on any web sites that it maintains that provides information about its customer services or benefits, and make the notice available electronically through the web site.
6. When providing the notice to an individual by e-mail, OHCA Members will:
- (a) ensure that the individual has agreed to electronic notice and such agreement has not been withdrawn;
  - (b) Provide a paper copy of the notice to the individual if OHCA Members know that an e-mail transmission of the electronic notice has failed.
7. OHCA Members will document compliance with and maintain the notice, or joint notice as applicable, by retaining copies of the notices issued by OHCA Members for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.
8. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **XIII. BUSINESS ASSOCIATES**

### **A. Relationships with Business Associates**

**Effective April 14, 2003**

#### **Purpose**

HIPAA provides that protected health information may be disclosed to business associates only if OHCA Members receive satisfactory assurances that the business associate will safeguard the privacy of the protected health information that such business associate creates or receives. A business associate is any person or entity that performs or helps to perform any function or activity that involves the use or disclosure of protected health information.

#### **Policy**

1. OHCA Members will receive satisfactory assurances from each business associate that such business associate will safeguard the privacy of the protected health information that it creates or receives.
2. OHCA Members will enter into appropriate business associate contracts with each business associate no later than April 14, 2004 or earlier, if required under the HIPAA Regulations if a service agreement with a business associate is entered into or renegotiated prior to April 14, 2004.

#### **Procedure**

1. Satisfactory Assurances must include contract provisions that:
  - Identify the uses and disclosures of protected health information permitted under the contract;
  - Permit the business associate to use or disclose the information only as permitted under the privacy rules;
  - Restrict the use and disclosure of protected health information that the business associate creates or receives to those specified in the contract;
  - Require the business associate to establish and use safeguards to prevent use and disclosure other than as specified in the business associate contract or as allowed by the HIPAA privacy rules;
  - Provide for the business associate to report any unauthorized use or disclosure to OHCA Members;
  - Require the business associate to apply the same restrictions and conditions on the use and disclosure of protected health information to the agents and subcontractors to whom it forwards the protected health information;
  - Make protected health information available to individuals;
  - Amend protected health information that it receives when asked to do so by OHCA Members;



- Make available to OHCA Members the information it needs to account for uses and disclosures of protected health information;
  - Make internal practices, books and records that are related to the use and disclosure of protected health information available to HHS for purposes of determining compliance with the privacy standards;
  - Return, if feasible, all protected health information to OHCA Members upon termination of the contract and destroy copies of such information. When return and/or destruction of protected health information is not feasible, the business associate will continue to apply the above-described privacy safeguards as set forth in the business associate contract to the uses and disclosures of such information for the purposes that make its return or destruction not feasible; and
  - Provide for the termination of the contract if the business associate violates the contractual provisions.
2. OHCA Members will enter into appropriate business associate contracts with each business associate no later than April 14, 2004 or earlier, if required under the HIPAA Regulations if a service agreement with a business associate is entered into or renegotiated prior to April 14, 2004 but after October 15, 2002.

## **B. Investigation and Correction of Business Associate Contractual Breaches**

**Effective April 14, 2003**

### **Purpose**

HIPAA provides that protected health information may be disclosed to business associates only if OHCA Members receive satisfactory assurances that the business associate will safeguard the privacy of the protected health information that such business associate creates or receives. When it is discovered by OHCA Members that the business associate has violated the terms of the business associate contract, steps must be taken to correct violations of the contractual provisions when the covered entity becomes aware of them.

### **Policy**

When the Privacy Officer is notified that a business associate has violated a material provision of the business associate contract related to the privacy of protected health information or has engaged in a pattern of activities or practices that constitute a material breach of the business associate contract, the Privacy Officer must take appropriate steps to correct the violation.

### **Procedure**

1. If a workforce member of OHCA Members becomes aware of activities or practices by a business associate that violate the terms of the business associate contract, such activities or practices must be reported to the Privacy Officer.
2. The Privacy Officer will contact the business associate and determine whether a contractual provision has been violated.
3. If a contract provision has been violated, the Privacy Officer will identify steps to be taken by the business associate that will enable the business associate to comply with its contractual obligations.
4. The Privacy Officer will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If an agreement can be reached, the corrective measures will be summarized in writing and sent to the business associate.
5. The business associate will provide the Privacy Officer with satisfactory assurances that appropriate corrective actions have been taken and that contract provisions will be complied with in the future.
6. If it is not possible to develop an acceptable corrective action plan, the Privacy Officer should take appropriate measures to terminate the contract.

## **C. Reporting of Contractual Breaches by Business Associates**

**Effective April 14, 2003**

### **Purpose**

HIPAA requires termination of a business associate contract when it is not possible to end the violation of the contractual obligation. HIPAA also requires a covered entity to report business associate contract violations to HHS when it is not possible to terminate the business associate contract.

### **Policy**

When it is not possible to end a violation of a contractual obligation of a business associate, OHCA Members shall terminate the business associate contract or if termination of the contract is not possible, OHCA Members shall report such business contract violation to HHS.

### **Procedure**

When the Privacy Officer is not able to correct violations of contractual obligations of a business associate, the Privacy Officer shall take the following steps:

1. Locate an alternate source for the services provided by the business associate;
2. Take formal action to terminate the business associate contract, including the notification of the business associate of such termination;
3. Arrange for a replacement of the business associate when the contract is formally terminated.
4. If the contract cannot be terminated, the contract violation should be reported by the Privacy Officer to HHS.

## **XIV. POLICY ON USE OF PHI FOR MARKETING**

**Effective: April 14, 2003**

### **Purpose**

This policy establishes guidelines for the use of Protected Health Information in marketing activities. Marketing is defined as a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing also includes an arrangement between a covered entity and any other entity whereby the health care provider or health plan discloses protected health information to the other entity, in exchange for direct or indirect 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

### **Policy**

1. OHCA Members will refrain from engaging in marketing activities unless it obtains an authorization from affected individuals authorizing the use or disclosure of protected health information for marketing purposes.
2. Marketing does not include communications that are made by a covered entity:
  - (a) For the purpose of describing 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
    - (1) the entities participating in a health care provider network or health plan network;
    - (2) replacement of, or enhancements to, a health plan; and
    - (3) 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;
  - (b) To an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or
  - (c) To an individual in the course of managing or coordinating the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

### **Procedure**

1. OHCA Members will obtain an individual's authorization for use or disclosure of protected health information for marketing unless the marketing communication:
  - Occurs in a face-to-face meeting with the individual, or

- Concerns promotional gifts of nominal value.
2. If OHCA Members are to receive direct or indirect remuneration in connection with the marketing communication, this fact must be stated on the authorization obtained from the individual.

## **XV. INDIVIDUALS' RIGHTS UNDER HIPAA**

### **A. Requesting Restrictions on Uses and Disclosures**

**Effective: April 14, 2003**

#### **Purpose**

HIPAA requirements provide an individual with the right to request restrictions to the use and disclosure of his or her protected health information. While covered entities are not required to permit the requested restrictions, they are required to permit the request. If the covered entity agrees to the requested restrictions, the covered entity may not make uses or disclosures that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law.

#### **Policy**

1. OHCA Members will allow an individual to request that uses and disclosures of his or her protected health information be restricted.

#### **Procedure**

1. OHCA Members will allow an individual to request to restrict the use and disclosure of protected health information for treatment, payment and health care operations. An individual may also request restrictions on the use and disclosure of protected health information covered by an authorization form.
2. The Privacy Officer is authorized to decide whether to agree to the requested restriction.
3. Upon agreeing to such a restriction, OHCA Members will not violate such restriction, unless as specified within this policy and procedure.
4. OHCA Members are not required to honor an individual's request in the following situation(s):
  - (a) when the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment;
  - (b) if restricted protected health information is disclosed to a health care provider for emergency treatment, OHCA Members will request that such health care provider not further use or disclose the information.
5. If an OHCA Member agrees to an individual's requested restriction, the restriction does not apply to the following uses and disclosures:
  - (a) to an individual accessing his or her own protected health information (see Policy entitled "Granting Access to Inspect and Obtain a Copy");

- (b) to an individual requesting an accounting of his or her own protected health information (see Policy entitled "Accounting of Disclosures");
  - (c) disclosures to Health and Human Services and instances for which an authorization or opportunity to agree or object is not required, such as judicial and administrative purposes; health oversight; research; law enforcement; public health; to avert a serious threat to health and safety; cadaveric organ, eye, or tissue donation; disclosures relating to decedents; Worker's Compensation; victims of abuse, neglect, or domestic violence; specialized government functions; or as required by law.
6. An OHCA Member may terminate its agreement to a restriction in the following situations:
- (a) the individual agrees to or requests the termination in writing;
  - (b) the individual orally agrees to the termination and the oral agreement is documented;
  - (c) the OHCA Member informs the individual that it is terminating its agreement to a restriction. Such termination is only effective with respect to protected health information created or received after it has so informed the individual.
7. OHCA Members will document and retain the restriction for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

## **B. Requests for Confidential Communications for PHI**

**C. Effective:** April 14, 2003

### **Purpose**

It is important to ensure that individuals can receive communications regarding their protected health information in a means and location that the individual feels is safe from unauthorized use or disclosure. A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations if the individual states that the disclosure of all or part of that information could endanger the individual. A health plan may agree to accommodate reasonable requests by individuals even if such requests would not meet the endangerment standard.

### **Policy**

1. OHCA Members will take necessary steps to accommodate reasonable requests by individuals to receive confidential communications of protected health information.
2. In complying with Policy 1, OHCA Members will provide confidential communications by alternative means or at alternative locations, without regard to whether disclosure of the information could endanger the individual.

### **Procedure**

1. OHCA Members may require individuals to make a request for a confidential communication in writing. If writing is not required, any oral request shall be documented by organization.
2. OHCA Members 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.
3. When appropriate, OHCA Members may condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.
4. An alternative means or location will be designated on a case by case basis, that is satisfactory to both OHCA Members and the individual before communication of protected health information is made.
5. The Privacy Officer, using professional judgment and considering all relevant factors, will be responsible for deciding the alternative means or location to communicate protected health information to an individual.
6. Once it is determined that use or disclosure is appropriate, workforce personnel with appropriate clearance will access the individual's protected health information in accordance with the confidential communication request that has been approved.



7. The requested protected health information will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
8. Once it is determined that use or disclosure is appropriate, workforce personnel with appropriate clearance will access the individual's protected health information in accordance with the confidential communication request that has been approved.
9. Authorized benefits personnel will appropriately document the request and delivery of the protected health information.
10. In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
11. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **D. Granting Access to Inspect and Obtain a Copy**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members recognize that individual rights are a critical aspect of maintaining quality care and service, and are committed to allowing individuals to exercise their rights under 45 CFR §164.524, and other applicable federal, state, and/or local laws and regulations. To support this commitment, OHCA Members will maintain and update, as appropriate, written policies and procedures to provide guidance on employee and organizational responsibilities regarding the rights of individuals to access, inspect, and obtain a copy of their protected health information.

### **Policy**

1. OHCA Members will take necessary steps to address individual requests to access, inspect, and/or obtain a copy of protected health information that is maintained in a designated record set in a timely and professional manner.
2. An individual may request to access, inspect, and/or obtain a copy of his or her protected health information that is maintained in a designated record set.
3. Individuals do not have the right to access the following types of information:
  - (a) Psychotherapy notes;
  - (b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
  - (c) Protected health information that is:
    - (1) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. §263a, to the extent the provision of access to the individual would be prohibited by law; or
    - (2) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR §493.3(a)(2).
4. The following persons are responsible for receiving and processing requests for access to protected health information by individuals: (1) Privacy Officer, or (2) Assistant Privacy Officer.

### **Procedures**

1. Individuals must direct requests for access, inspection, or a copy of protected health information to the Assistant Privacy Officer or Privacy Officer and complete the form entitled "Request for Health Information".

2. The individual will be informed that request for access is required to be in writing.
3. An appropriate request from an individual regarding protected health information using form "Request for Health Information" will, within a reasonable time period, be reported, along with the form, to Health Benefits personnel with appropriate access clearance to protected health information.
4. Upon receipt of a request made, Health Benefits personnel with appropriate clearance will act on the request by:
  - (a) informing the individual of the acceptance and providing the access requested or
  - (b) providing the individual with a written denial.

To determine whether a request should be denied, see Policy entitled "Denying Access to Inspect and Obtain a Copy of Protected Health Information", and policy entitled "Reviewing a Denial to Access to Protected Health Information."

5. Action taken pursuant to Procedure 4 must be taken:
  - (a) no later than 30 days after the request is made; or,
  - (b) if the request is for protected health information that is not maintained or accessible on-site to OHCA Members, no later than 60 days after the request.
6. If OHCA Members cannot take action on a request for access to protected health information within the relevant time periods listed in Procedure 5; OHCA Members may extend the time required by 30 days (see policy entitled "Extending Time to Access").
7. Health Benefits personnel with appropriate access clearance will access the individual's protected health information using proper access and authorization procedures.
8. The individual will be allowed access, inspection, and/or copies of the requested protected health information in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
9. OHCA Members will provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format.
10. If the requested format is not readily producible, then OHCA Members will provide the individual with access to the protected health information in a readable hard copy form or such other form as agreed to by the individual.
11. If requested by the individual, OHCA Members will arrange with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing of protected health information, within the specified time period.

12. A summary of the requested protected health information will be provided in lieu of access to the information only when the individual agrees in advance to a summary, and to any related fees imposed.
13. An explanation of the requested protected health information to which access has been provided will accompany the access only when the individual agrees in advance to a summary, and to any related fees imposed.
14. If a summary or explanation of the requested information is to be prepared, such summary or explanation will be completed only by Health Benefits personnel, or other applicable personnel with appropriate access clearance.
15. The Assistant Privacy Officer or Privacy Officer will appropriately document the request and delivery of the protected health information.
16. Any fees imposed on the individual for a copy of the protected health information or a summary or explanation of such information will:
  - (a) be collected by the Assistant Privacy Officer or Privacy Officer at the time of receipt of the request and the proper completion of the request form.
  - (b) be reasonable and cost-based;
  - (c) will be only for the cost of the following:
    - (1) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual,
    - (2) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
    - (3) Preparing an explanation or summary of the protected health information.
    - (4) No fees shall apply for the cost associated with searching and retrieving the requested information.
17. OHCA Members will document and retain designated record sets that are subject to access by individuals for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.
18. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **E. Denying Access to Inspect and Obtain a Copy of PHI**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members recognize that individual rights are a critical aspect of maintaining quality care and service, and are committed to allowing individuals to exercise their rights under 45 CFR §164.524, and other applicable federal, state, and/or local laws and regulations. To support this commitment, OHCA Members will maintain and update, as appropriate, written policies and procedures to provide guidance on employee and organizational responsibilities with respect to the rights of individuals regarding their protected health information.

Situations may arise when the Privacy Officer must make a determination to deny an individual access to their protected health information, in accordance with applicable laws and regulations. The policies and procedures herein have been established to assist personnel in evaluating the appropriateness of such a determination. Personnel should also refer to the Policy entitled "Granting Access to Inspect and Obtain a Copy" in responding to an individual's request for access to protected health information.

### **Policy**

1. OHCA Members will take necessary steps to address individual requests to access, inspect, and/or obtain a copy of protected health information that is maintained in a designated record set in a timely and professional manner.
2. OHCA Members will adhere to the procedures herein when denying access to inspect or obtain a copy of protected health information.

### **Procedures**

1. Upon receipt of a request made to access, inspect or copy protected health information, Health Benefits personnel with appropriate clearance will act on the request by (1) informing the individual of the acceptance and providing the access requested (see Policy entitled "Granting Access to Inspect and Obtain a Copy"); or (2) providing the individual with a written denial.
2. Action taken pursuant to procedure 1 must be taken:
  - (a) no later than 30 days after the request is made; or,
  - (b) if the request is for protected health information that is not maintained or accessible on-site to OHCA Members, no later than 60 days after the request is made.
3. If OHCA Members cannot take action on a request for access to protected health information within the relevant time periods listed in procedure 1, OHCA Members may extend the time required by 30 days [see policy entitled "Extending Time to Access"].

4. A denial of access will be issued and will not be reviewed in the following circumstances:
  - (a) the protected health information is:
    - (1) Psychotherapy notes;
    - (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
    - (3) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 USC §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, pursuant to 42 CFR §493.3(a)(2).
  - (b) the individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 USC §552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law;
  - (c) the individual's access may be denied if the protected health information 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.
5. If an individual has been denied access to protected health information, the OHCA Members will review a denial for access to protected health information when requested by an individual in the following situations:
  - (a) 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) the protected health information 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) 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.
6. See Policy entitled "Reviewing a Denial to Access Protected Health Information" for reviewing a denial to access protected health information.
7. In denying access in whole or in part, to the extent possible, Health Benefits personnel will give the individual access to any other protected health information requested, after excluding the protected health information that was denied.

8. When denying an individual access to protected health information, the denial will:
  - (a) be written in plain language;
  - (b) contain the basis for the denial;
  - (c) contain the following statement, if applicable (only if review is allowed by Procedure 5 above):

THE INDIVIDUAL HAS THE RIGHT TO HAVE THE DENIAL REVIEWED BY A LICENSED HEALTH CARE PROFESSIONAL, DESIGNATED BY OHCA MEMBERS TO ACT AS A REVIEWING OFFICIAL AND WHO DID NOT PARTICIPATE IN THE ORIGINAL DENIAL DECISION. INDIVIDUALS MAY EXERCISE THEIR REVIEW RIGHTS BY SUBMITTING A WRITTEN REQUEST TO THE OHCA MEMBER.

- (d) contain a description of how the individual may complain to OHCA Members pursuant to its complaint procedures or to the HHS Secretary.
9. The description of how the individual may complain will include the name, or title, and telephone number of the contact person or office designated to receive such complaints.
10. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **F. Reviewing a Denial to Access PHI**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members recognize that individual rights are a critical aspect of maintaining quality service, and is committed to allowing individuals to exercise their rights under 45 CFR §164.524, and other applicable federal, state, and/or local laws and regulations. To support this commitment, OHCA Members will maintain and update, as appropriate, written policies and procedures to provide guidance on employee and organizational responsibilities with respect to the rights of individuals regarding their protected health information. However, situations may arise when the Privacy Officer must make a determination to deny an individual access to their protected health information, in accordance with applicable laws and regulations. In certain circumstances, individuals may request that the denial be reviewed. The policies and procedures herein have been established to assist personnel in such a review. Personnel should also refer to the Policies entitled "Granting Access to Inspect and Obtain a Copy" and "Denying Access to Inspect and Obtain a Copy of Protected Health Information" in responding to an individual's request for access to protected health information.

### **Policy**

1. OHCA Members will take necessary steps to address individual requests to access, inspect, and/or obtain a copy of protected health information that is maintained in a designated record set in a timely and professional manner.
2. OHCA Members will adhere to procedures set forth herein when denying access, inspection, or copying of protected health information.
3. OHCA Members will adhere to the following procedures when reviewing a denial to access protected health information

### **Procedures**

1. OHCA Members will review a denial for access to protected health information when requested by the individual, in the following situations:
  - (a) 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) the protected health information 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) 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.

2. All denial reviews will be conducted by a licensed health care professional who is designated by OHCA Members to act as a reviewing official and who did not participate in the original decision to deny.
3. The designated reviewing official will be determined on a case by case basis by the Privacy Officer.
4. Health Benefits personnel will promptly refer a request for review to the designated reviewing official.
5. The designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested based on the applicable standards.
6. Health Benefits personnel will promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required to carry out the designated reviewing official's determination.
7. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer, Assistant Privacy Officer or to the employee compliance hotline.

## **G. Accepting Requests for Amendments to PHI**

**Effective: April 14, 2003**

### **Purpose**

Under HIPAA, individuals have the right to request an amendment or correction to their protected health information. Entities have the right to deny the request to amend or correct protected health information. Unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment, this provision applies to protected health information created by the covered entity. For both of those situations, OHCA Members have created policies and procedures to address the issue and to comply with any applicable laws.

### **Policy**

1. OHCA Members will provide for an individual to request an amendment to his or her protected health information or a record in a designated record set for as long as the information is maintained in the designated record set.
2. OHCA Members will allow an individual's request to amend protected health information that was not created by OHCA Members if provided a reasonable basis to believe that the originator of the information is no longer available to act on the request.

### **Procedure**

1. The Privacy Officer or Assistant Privacy Officer will be responsible for receiving, processing, and responding to requests for amendments to protected health information.
2. All individual requests for amendments to protected or other health information will be in writing, and directed to the Privacy Officer or Assistant Privacy Officer.
3. The Privacy Officer or Assistant Privacy Officer will inform the individual that it requires individuals to make requests for amendments in writing.
4. Individuals must document the reason(s) to support the requested amendment.
5. The request may be referred to a designated health care professional for review, who will be selected by the Privacy Officer or Assistant Privacy Officer on a case by case basis.
6. An individual's request for amendment may be denied if the requested protected health information or record:
  - (a) was not created by OHCA Members;
  - (b) is not part of the designated record set;

- (c) would not be available for inspection under the requirements for individual rights to access protected health information; or
  - (d) is accurate and complete.
- 7. If the requested amendment is denied, see Policy entitled "Denying Requests for Amendments to PHI".
- 8. The Privacy Officer or Assistant Privacy Officer will inform the individual no later than 60 days after receipt of such a request if the amendment is accepted.
- 9. The time period for the action by OHCA Members will be extended by no more than 30 days.
- 10. If the time period for the action is extended, the Privacy Officer or Assistant Privacy Officer will, within 30 days after receipt of the request, provide the individual with a written statement of the reasons for the delay and the date by which OHCA Members will complete the action on the request.
- 11. The time period for action will not be extended more than once.
- 12. If the requested amendment is accepted, the Privacy Officer or Assistant Privacy Officer will:
  - (a) make the appropriate amendment; or
  - (b) arrange to have the necessary health care professional make the amendment.
- 13. Upon accepting and completing a requested amendment, the Privacy Officer or Assistant Privacy Officer will perform the following tasks:
  - (a) inform the individual, in a timely manner, and obtain the individual's identification of and agreement to have OHCA Members notify the relevant persons with which the amendment needs to be shared;
  - (b) make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as needing the amendment;
  - (c) make reasonable efforts to inform and provide the amendment within a reasonable time to persons, including business associates, that OHCA Members know have the affected protected health information and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.
- 14. In completing the amendment the Privacy Officer or Assistant Privacy Officer will, at a minimum, identify the affected information in the designated record set and append or otherwise provide a link to the location of the amendment.

15. In the event that another covered entity notifies OHCA Members of an amendment to an individual's protected health information, the Privacy Officer or Assistant Privacy Officer will amend the respective information by, at minimum, identifying the affected information in the designated record set and appending or otherwise providing a link to the location of the amendment.

## **H. Denying Requests for Amendments to PHI**

**Effective: April 14, 2003**

### **Purpose**

Under HIPAA, individuals have the right to request an amendment or correction to their protected health information, or a record about the individual for as long as that information is contained in a designated record set. Entities have the right to deny the request to amend or correct protected health information. Unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment, this provision applies to protected health information created by the covered entity. OHCA Members have created policies and procedures to address this issue and to comply with any applicable laws.

### **Policy**

1. OHCA Members permit for an individual to request an amendment or correction to his or her protected health information or a record in a designated record set for as long as the information is maintained in the designated record set.
2. OHCA Members may deny an individual's request for amendment if it determines that the requested protected health information or record:
  - (a) was not created by OHCA Members, unless the individual provides a reasonable basis to believe that the originator of protected health information 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 requirements for individual rights to access protected health information [see the Policy entitled "Granting Access to Inspect and Obtain a Copy"]; or
  - (d) is accurate and complete.

### **Procedure**

1. The Privacy Officer or Assistant Privacy Officer will be responsible for receiving, processing, and responding to requests for amendments to protected health information.
2. The review of a request for an amendment or correction to protected health information will be conducted in accordance with the Policy entitled "Accepting Requests for Amendments to PHI."
3. The Privacy Officer or Assistant Privacy Officer will inform the individual no later than 60 days after the individual's request if the amendment is denied.

4. On occasions where OHCA Members need more than 60 days to make a decision, the time period for the action will be extended by no more than 30 days provided that:
  - (a) OHCA Members provide the individual with a written statement of the reasons for the delay and the date by which OHCA Members will complete the action on the request; and
  - (b) OHCA Members extend the time period for action not more than once.
5. Upon denying an amendment, in whole or in part, OHCA Members will provide the individual with a written denial in accordance within the timeframes outlined in procedures 3 and 4.
6. The denial will be written in plain language and will contain the following:
  - (a) the basis for the denial (see policy 2 above);
  - (b) the individual's right to submit a written statement disagreeing with the denial;
  - (c) a description of how the individual may file such a statement;
  - (d) a description of how the individual may file a complaint to OHCA Members pursuant to its complaint procedures including the name, or title, and telephone number of the contact person or office designated to receive such complaints;
  - (e) a description of how the individual may file a complaint with the Department of Health and Human Services ("HHS");
  - (f) the following statement:

IF THE INDIVIDUAL DOES NOT SUBMIT A STATEMENT OF DISAGREEMENT, THEN THE INDIVIDUAL MAY REQUEST OHCA MEMBERS TO PROVIDE THE INDIVIDUAL'S REQUEST FOR AMENDMENT AND THE DENIAL WITH ANY FUTURE DISCLOSURES OF THE PROTECTED HEALTH INFORMATION THAT IS THE SUBJECT OF THE AMENDMENT.
7. If the individual provides a statement of disagreement, OHCA Members may prepare a written rebuttal to the individual's statement of disagreement.
8. OHCA Members will provide the individual with a copy of the above rebuttal.
9. OHCA Members will append or otherwise link the following to the designated record set or protected health information that is the subject of the disputed amendment:
  - (a) the individual's request for an amendment;
  - (b) the denial of the request;
  - (c) the individual's statement of disagreement, if any; and

- (d) OHCA Members' rebuttal, if any.
10. Any subsequent disclosures of the protected health information to which an individual's written disagreement relates will include the following:
    - (a) the material appended as described above; or
    - (b) an accurate summary of any such information.
  11. Subsequent disclosures may be transmitted separately from a standard transaction if the standard transaction does not allow the information in Procedure 9 to be transmitted.
  12. If the individual has not submitted a written statement of disagreement, OHCA Members will include the individual's request for amendment and OHCA Members' denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action.

## **I. Accounting of Disclosures**

**Effective: April 14, 2003**

### **Purpose**

HIPAA requires that individuals have a right to receive an accounting of various instances when protected health information about them is disclosed by a covered entity, subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies. OHCA Members have developed policies and procedures to address the accounting of instances when protected health information has been used or disclosed for purposes other than treatment, payment, or health care operations.

### **Policy**

1. OHCA Members will allow individuals to receive an accounting of all instances, subject to certain limitations described below, where protected health information about them is used or disclosed.
2. OHCA Members will allow individuals to receive an accounting of instances where protected health information about them is used or disclosed, except for the following purposes:
  - (a) to carry out treatment, payment and health care operations;
  - (b) to the individuals of protected health information about themselves;
  - (c) pursuant to an authorization;
  - (d) incident to a use or disclosure otherwise permitted or required by the privacy rules;
  - (e) as part of a limited data set under 45 CFR 164.514(e);
  - (f) to persons involved in the individual's care or other notification purposes;
  - (g) for national security or intelligence purposes;
  - (h) to correctional institutions or law enforcement custodial situations.
3. OHCA Members will not allow individuals to receive an accounting of instances where protected health information about them is used or disclosed prior to April 14, 2003.
4. OHCA Members will document and maintain an accounting of when individual's protected health information has been disclosed for purposes other than those described in Procedure 2 [see Policy entitled "Maintaining Appropriate Documentation Regarding Compliance with HIPAA Privacy Requirements].



## Procedure

1. OHCA Members will allow an individual to obtain an accounting of instances when their protected health information has been disclosed.
2. OHCA Members will allow an individual to receive an accounting of disclosures of protected health information made by OHCA Members in the six years prior to the date on which the accounting is requested; provided, however, that no accounting of disclosures will be provided that occurred prior to April 14, 2003.
3. The accounting will be in writing and will include disclosures made to or by business associates of OHCA Members.
4. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.
5. Each accounting of a disclosure will include the following:
  - (a) the date of disclosure;
  - (b) the name of the entity or person who received the protected health information and, if known, the address of such entity or person;
  - (c) a brief description of the protected health information disclosed;
  - (d) 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
    - (1) a copy of a written request for a disclosure from an entity in which an individual's authorization is not required under 45 CFR 164.512; or
    - (2) a copy of a written request for a disclosure required by the HHS Secretary to investigate or determine the covered entity's compliance with applicable laws and regulations.
6. If OHCA Members have made multiple disclosures of protected health information to the same person or entity for a single purpose under 45 CFR 164.502(a)(2)(ii) (disclosures required by HHS to investigate or determine the covered entity's compliance with applicable laws and regulations) or 45 CFR 164.512 (uses and disclosures of protected health information in which an individual's authorization is not required), the accounting may, with respect to multiple disclosures, provide:
  - (a) the information required by Procedure 4 for the first disclosure during the accounting period;
  - (b) the frequency, periodicity or number of the disclosures made during the accounting period; and

- (c) the date of the last such disclosure during the accounting period.
7. OHCA Members will act on the individual's request for an accounting not later than 60 days after receipt of the request by
    - (a) providing the individual with the accounting requested, or
    - (b) extending the time to provide the accounting by no more than 30 days.
  8. In the event that OHCA Members extend the time to provide the accounting, within 60 days after receipt of the request, it will provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting.
  9. OHCA Members will not extend the time to provide the accounting more than once.
  10. The first accounting to an individual in any 12 month period will be without charge.
  11. Any fee imposed by OHCA Members for each subsequent request for an accounting by the same individual within the 12 month period will be cost-based.
  12. Upon imposing a fee OHCA Members will inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
  13. OHCA Members will document and retain the following for a period of at least 6 years, or from the date of its creation or the date when it last was in effect, whichever is later:
    - (a) the information required to be included in an accounting;
    - (b) the written accounting that is provided to the individual;
    - (c) the title of the persons or officer responsible for receiving and processing requests for an accounting by individual.
  14. The Privacy Officer is responsible for responding to a request from an individual for an audit trail of instances when their protected health information has been disclosed for purposes other than those set forth in Policy 2 above.

## **J. Individual Rights to File Complaints**

**Effective: April 14, 2003**

### **Purpose**

HIPAA requires covered plans and providers to have a mechanism for receiving complaints from individuals regarding the covered entity's compliance with the requirement of the Privacy standards. The covered entity is required to accept complaints about any aspect of their practices regarding protected health information. For example, individuals would be able to file a complaint when they believe that protected health information relating to them has been used or disclosed improperly; that an employee of the entity has improperly handled the information; that they have wrongfully been denied access to or opportunity to amend the information; or, that the entity's notice does not accurately reflect its information practices.

### **Policy**

1. As specified in 45 CFR §164.530(d), OHCA Members will provide a process for individuals to make complaints concerning OHCA Members' policies and procedures regarding the use or disclosure of protected health information, or its compliance with such policies and procedures.
2. The Privacy Officer and Assistant Privacy Officer will be OHCA Members' designated contact for individuals to file complaints pursuant to this policy.
3. OHCA Members will not require individuals to waive their rights to file a complaint with the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

### **Procedure**

1. OHCA Members will document all complaints received, and their disposition, if any, for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.
2. The Privacy Officer should be contacted in order to file complaint concerning OHCA Members' policies and procedures required by the HIPAA privacy rule, or their compliance with such policies and procedures.
3. The name, or title, and telephone number of the contact person or office designated to receive complaints concerning OHCA Members' policies and procedures required by the HIPAA privacy rule, or its compliance with such policies and procedures will be documented.

## **XVI. SANCTIONING OF WORKFORCE**

**Effective: April 14, 2003**

### **Purpose**

OHCA Members have established and will apply appropriate sanctions against members of their workforce who fail to comply with their policies and procedures. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctioning for violating OHCA Members' policies and procedures. Under the Health Insurance Portability and Accountability Act, penalties for misuse or misappropriation of health information include both civil monetary penalties and criminal penalties.

### **Policy**

1. OHCA Members will apply appropriate sanctions against members of their workforce who fail to comply with the OHCA Members policies and procedures.
2. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.
3. Workforce members should be aware that violations of a severe nature may result in notification to law enforcement officials.
4. The policy and procedures contained herein do not apply specifically when members of OHCA Members' workforce exercise their right to:
  - (a) file a complaint with HHS;
  - (b) testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI;
  - (c) oppose any act made unlawful by the HIPAA privacy rule; provided the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy rule;
  - (d) disclose protected health information as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individuals legal options with regard to the whistleblower activity; or
  - (e) disclose protected health information to a law enforcement official when an employee is a victim of a crime, provided that the protected health information is about a suspected perpetrator of the criminal act; and is limited to the information

listed in the Policy relating to Disclosing Protected Health Information for Law Enforcement Release.

## Procedures

1. All workforce members shall report possible violations of privacy practices and procedures to the Privacy Officer.
2. Upon being notified of a potential violation of the privacy rules, the Privacy Officer will
  - review any documentation that has been prepared;
  - meet with the individual who reported the possible violation;
  - meet with the individual who may have violated the policies and procedures;
  - determine what, if any, protected health information was used or disclosed and if so, whether such use or disclosure violated the policies and procedures;
  - determine whether the violation was accidental or intentional;
  - recommend the disciplinary action, if any, that should be taken; and
  - document the findings of the investigation and the action taken.
3. If a workforce member is found to have *intentionally* violated the privacy policies and procedures, such violation may result in the immediate suspension pending further investigation and subsequent termination or any other reasonable action at the discretion of the Privacy Officer based upon all relevant facts and circumstances and as appropriate to the particular situation, including notification to law enforcement officials. Documentation of the investigation of the violation must show clear evidence that the disclosure was intentional and deliberate and such workforce member knew that the action violated the policies and procedures as set forth in this manual.
4. If a workforce member is found to have *unintentionally* violated a privacy rule or used or disclosed protected health information in violation of the privacy policies and procedures, such workforce member shall:
  - (a) First Offense of Noncompliance: The workforce member shall meet with the Privacy Officer and such member's Department Director to review the violation and demonstrate to the satisfaction of the Privacy Officer that he or she understands the uses and disclosures that he or she is authorized to make under the policies and procedures and the HIPAA privacy rules; provided, however, that the workforce member's Department Director shall not receive any form of protected health information.
  - (b) Second Offense of Noncompliance: The workforce member shall meet with the Privacy Officer and such workforce member's Department Director to review the violation and shall receive a written reprimand to be filed in such workforce member's personnel file; provided, however, that the workforce member's Department Director shall not receive any form of protected health information. The workforce member must again demonstrate to the satisfaction of the Privacy Officer that he or she understands the uses and disclosures that he or she is

authorized to make under the policies and procedures and the HIPAA privacy rules.

- (c) Subsequent Offenses: Upon commission of the third or any subsequent offense, the workforce member shall meet with the Privacy Officer and such member's Department Director to review the violation and shall receive a written reprimand to be filed in such workforce member's personnel file; provided, however, that the workforce member's Department Director shall not receive any form of protected health information. A pattern of repeated violations may result in the suspension or termination of the workforce member at the discretion of the Privacy Officer based upon the facts and circumstances of the particular violation.
5. The Privacy Officer is responsible for determining the severity of sanctions necessary.
  6. Notwithstanding anything to the contrary, except as may otherwise be required by the HIPAA rules and regulations, punishments for failure(s) (either unintentional or intentional) to comply with the policies or procedures set forth in this manual or with the requirements of HIPAA regulations shall be consistent with and in accordance with the normal disciplinary procedures of the City of Corpus Christi, which may include, but are not limited to, suspension or termination of employment.
  7. All sanctioning of employees will be documented and retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later. An unproven or unsubstantiated allegation of a violation does not need to be documented.

## **XVII. MITIGATION OF VIOLATIONS**

**Effective: April 14, 2003**

### **Purpose**

45 CFR 164.530(f) requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of the privacy rule by the covered entity or its business associates.

### **Policy**

It is the policy of OHCA Members to mitigate, to the extent practicable based upon the applicable facts and circumstances, any harmful effect known to OHCA Members of a violation of the privacy rules or a violation of this manual.

### **Procedures**

1. All workforce members of the Plan Sponsor shall immediately notify the Privacy Officer upon learning of a violation of the privacy rule or the policies and procedures set forth in this manual.
2. Upon determining that an OHCA Member, a workforce member of the Plan Sponsor or a business associate of OHCA Members have made a use or disclosure of protected health information that violates the privacy rules or the policies and procedures set forth in this manual, the Privacy Officer shall determine any action needed to mitigate any harm to the individual whose information was used or disclosed based upon the applicable facts and circumstances.
3. The Privacy Officer shall document the violation and the course of action taken to mitigate the violation.

## **XVIII. MAINTAINING APPROPRIATE DOCUMENTATION REGARDING COMPLIANCE WITH HIPAA PRIVACY REQUIREMENTS**

**Effective: April 14, 2003**

### **Purpose**

This policy is designed to give guidance and ensure compliance with provisions of HIPAA requiring covered entities to maintain documentation of policies, procedures, and other administrative documents.

### **Policy**

1. OHCA Members will implement policies and procedures with respect to protected health information, that are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy regulations.
2. OHCA Members will maintain documentation, in written or electronic form, of policies, procedures, communications, and other administrative documents as required by 45 CFR §164.530(i) and (j), for a period of at least six years from the date of creation or the date when last in effect, whichever is later.
3. OHCA Members will incorporate into their policies, procedures and other administrative documents any changes in law.
4. OHCA Members will properly document and implement any changes to policies and procedures as necessary by changes in law.

### **Procedures**

1. OHCA Members' policies have been reasonably designed to take into account the size and type of activities undertaken by OHCA Members with respect to protected health information.
2. The Privacy Officer shall have overall responsibility for establishing a system to ensure documentation of actions required in this policy and procedure manual.
3. In implementing a change in Privacy Practices, OHCA Members will:
  - Ensure that the policy or procedure, as revised to reflect a change in OHCA Members' privacy practice, complies with the standards, requirements, and implementation specifications of the Privacy regulations;
  - Document the policy or procedure as revised;
  - Revise the Notice of Privacy Practices to state the changes in practice and make the revised notice available [see policy entitled "Notice of Privacy Practices - Content of Notice"]; and



- OHCA Members will not implement a change in policy or procedure prior to the effective date of the revised notice.
4. OHCA Members may change policies or procedures that do not affect the content of the Notice of Privacy Practices, provided that the policy or procedure complies with the privacy regulations and is documented as required in this policy.
  5. The following documentation will be maintained in an organized manner:
    - policies and procedures set forth in this manual;
    - forms for the authorization to use or disclose protected health information and any revocations thereof;
    - requests for an accounting of disclosures of protected health information and all records related to such requests;
    - requests for restrictions on uses and disclosures and requests for confidential communications and all revocations thereof;
    - records for amendment of protected health information and records related to the disposition of such requests;
    - agreements with business associates referring to the use or disclosure of protected health information;
    - Notice of Privacy Practices and any changes made thereto;
    - records of disciplinary action taken against workforce members for violations of the privacy policies and procedures;
    - records of actions taken to enforce compliance with contract provisions by business associates
    - complaints received from individuals and associated written correspondence; and
    - permitted and required disclosures (other than for treatment, payment and health care operations) which are required to be documented.
  6. Documentation will be maintained in a manner that allows necessary availability, while also ensuring the security of information.