

City of Lakeland

**Health Insurance Portability and Accountability Act
(HIPAA)**

Privacy Use and Disclosure

Policy and Procedures

Table of Contents

| | |
|--|----------|
| Plan’s Responsibility as Covered Entity | 4 |
| 1. Privacy Official and Contact Person | 4 |
| 2. Workforce Training | 5 |
| 3. Technical and Physical Safeguards and Firewall..... | 5 |
| 4. Privacy Notice | 5 |
| 5. Complaints | 6 |
| 6. Sanctions for Violations of Privacy Policy | 6 |
| 7. Mitigation of Inadvertent Disclosures of Protected Health Information | 6 |
| 8. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy | 6 |
| 9. Plan Document..... | 7 |
| 10. Documentation..... | 7 |
| | |
| Policies on Use and Disclosure of PHI | 9 |
| 1. Use and Disclosure Defined..... | 9 |
| 2. Workforce Must Comply With City’s Policy and Procedures | 9 |
| 3. Access to PHI is Limited to Certain Employees..... | 9 |
| 4. Permitted Uses and Disclosures: Payment and Health Care Operations | 10 |
| 5. No Disclosure of PHI for Non-Health Plan Operations | 11 |
| 6. Mandatory Disclosures of PHI: To Individuals and DHHS..... | 11 |
| 7. Permissive Disclosures of PHI: For Legal and Public Policy Purposes | 11 |
| 8. Disclosures of PHI Pursuant to an authorization..... | 12 |
| 9. Complying With the “Minimum-Necessary” Standard | 12 |
| 10. Disclosures of PHI to Business Associates..... | 15 |
| 11. Disclosures of De-identified Information..... | 15 |

Table of Contents (Continued)

| | |
|---|-----------|
| Policies on Individual Rights..... | 16 |
| 1. Access to Protected Health Information and Requests for Amendment..... | 16 |
| 2. Accounting..... | 16 |
| 3. Requests for Alternative Communication Means or Locations..... | 17 |
| 4. Requests on Restrictions on Uses and Disclosures of PHI..... | 17 |
| | |
| Use and Disclosure Procedures | 18 |
| 1. Procedures for Use and Disclosure of PHI | 18 |
| 2. Mandatory Disclosures of PHI: to Individuals and DHHS..... | 19 |
| 3. Permissive Disclosures of PHI: for Legal and Public Policy Purposes..... | 19 |
| 4. Disclosures of PHI Pursuant to an Authorization | 21 |
| 5. Disclosures of PHI to Business Associates..... | 22 |
| 6. Requests for Disclosure of PHI from Spouse, Family Member, or Friend | 22 |
| 7. Disclosures of De-Identified Information | 23 |
| 8. Verification of Identity of Those Requesting PHI..... | 23 |
| 9. Complying With the "Minimum-Necessary" Standard..... | 25 |
| 10. Documentation..... | 26 |
| 11. Mitigation of Inadvertent Disclosures of PHI..... | 27 |
| | |
| Procedures for Complying With Individual Rights | 28 |
| 1. Individual's Request for Access | 28 |
| 2. Individual's Request for Amendment..... | 29 |
| 3. Processing Requests for an Accounting of Disclosures of PHI..... | 30 |
| 4. Processing Requests for Confidential Communications | 32 |
| 5. Processing Requests for Restrictions on Uses and Disclosures of PHI | 32 |
| | |
| Procedures to Safeguard PHI | 33 |

HIPAA Privacy Policy

Introduction

The City of Lakeland (the City) sponsors group health, pharmaceutical, dental, vision, Employee Assistance Program, and flexible spending plans referred to as (the Plan). Members of the City's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the City, for administrative functions of the Plan. In addition, certain employees of the City may receive or transmit individually identifiable health information in connection with the City's general operations and services.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the City's ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan or the City as an employer or health care provider and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the City's policy to comply fully with HIPAA's requirements. To that end, all members of the City's workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy, the City's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the City, whether or not they are paid by the City. The term "employee" includes all of these types of workers.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The City reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the City. This Policy does not address requirements under other federal laws or under state laws.

Plan's Responsibilities as Covered Entity

1. Privacy Official and Contact Person

The Health Benefits Coordinator will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the

City's use and disclosure procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The City's Privacy Official is Bryan Riley, Health Benefits Coordinator, Department of Risk Management.

Each of the following departments shall have a designated Privacy Coordinator:

- City Manager's Office
- Civil Service
- Electric
- Employee Relations
- Finance
- Fire
- Housing
- Internal Audit
- Police
- Records Retention

All privacy coordinators should meet on an annual basis or as needed with the Privacy Official to monitor ongoing compliance with this privacy policy.

2. Workforce Training

It is the City's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all affected workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plan.

3. Technical and Physical Safeguards and Firewall

The City will establish on behalf of the Plan appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

4. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights; and

- the Plan's legal duties with respect to the PHI.

The privacy notice will inform participants that the City will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the City's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- no later than April 14, 2003
- on an ongoing basis, at the time of an individual's enrollment in the Plan, and
- within 60 days after a material change to the notice

The Plan will also provide notice of availability of the privacy notice at least once every three years.

5. Complaints

Complaints shall be made to the Privacy Official, Bryan Riley, Office of Risk Management, 520 North Lake Parker Avenue, Lakeland, Florida 33801, Phone: 863-834-6795, and Fax: 863-834-6787.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

6. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with the City of Lakeland's Disciplinary Procedures as referenced in the Personnel Policy and Procedure Manual, up to and including termination.

7. Mitigation of Inadvertent Disclosures of Protected Health Information

The City shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a use or disclosure of protected health information, either by an employee of the City or an outside consultant/contractor, that is not in compliance with this Policy, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the participant can be taken.

8. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be

required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

9. Plan Document

The Plan document includes provisions describing the permitted and required uses and disclosures of PHI by the City for plan administrative purposes. Specifically, the Plan document requires the City to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the City;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures as required by law;
- make the City's internal practices and records relating to the use and disclosure of PHI received from the Plan available to Department of Health and Human Resources (DHHS) upon request; and
- if feasible, return or destroy all PHI received from the Plan that the City 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.

The Plan document also requires the City to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the City agrees to those restrictions; and (2) provide adequate safeguards.

10. Documentation

The Plan's and the City's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The Plan and the City shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years.

Policies on Use and Disclosure of PHI

1. Use and Disclosure Defined

The City and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- **Use.** The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the City of Lakeland, Office of Risk Management or other affected City Departments or by a Business Associate. Business Associates of the Plan or the City are as follows – United Healthcare, WHP Health Initiatives, Inc. d/b/a Walgreens Health Initiatives, Gallagher Benefit Services, Inc. a division of Arthur J. Gallagher and Company, Horizon Behavioral Services, Ross, Vecchio, and Trussell, P.A., Carter, Belcourt and Atkinson, P.A., C.P.A.
- **Disclosure.** For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the City of Lakeland, Office of Risk Management or other affected departments of the City.

2. Workforce Must Comply With City's Policy and Procedures

All members of the City's workforce (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and with the City's use and disclosure procedures, which are set forth in this document.

3. Access to PHI Is Limited to Certain Employees

The following below listed Departments and positions will have access to PHI on behalf of the City for its use in Plan Administration and will be limited to information necessary to initiate the function:

- Health Benefits Coordinator, Office Associate II, Director of Risk Management, Occupational Health Nurse, Administrative Assistant, who perform functions directly on behalf of the group health plan, and
- Account Clerk II, III, IV, Administrative Assistant, Assistant Fire Chief, Chief Information Security Officer, Assistant Police Chief, Clerk, Computer Applications Specialist, Crime Scene Technician I, II, Customer Service Representative I, II, Customer Service Coordinator, Directors, Driver Engineer, Employee Relations Specialist III, EMS Supervisor, Fire Chief, Engineering Technician I, II, III, IV, Fire Equipment Mechanic, Fire Lieutenant, Fire Marshall, Fire Safety Inspector, Fire Shift Commander, Fire Training Officer, GIS Technician II, Housing Division Manager, Housing Programs Coordinator, Housing Rehab Finance Officer I, II, Housing Rehab Specialist II, Internal Audit Manager, Internal Auditor I, Legal Secretary, Maintenance Supervisor, Managers, Master Police Officer, Office Assistant I, II, Office Associate I, II, III, Payroll Manager,

Payroll Supervisor, Planning Assistant, Police Captain, Police Chief, Police Lieutenant, Police Officer, Police Sergeant, Police Property Clerk, Property Information Supervisor, Public Education Officer, Public Safety Aide I, Records Supervisor, Safety Coordinator, Safety Manager, Safety Officer, Supervisors, Supervisor of Systems Control/Reliability, T & D Supervisor, Timekeepers/TES Users, Victim Assistant Advocate, and Victim Assistant Coordinator, who have access to PHI on behalf of the City for its use in plan administrative functions, as well as during the scope and course of their job related duties.

The same employees may be named or described in both of these two categories. These employees with access may use and disclose PHI for plan administrative functions, as well as during the scope and course of their job related duties, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the more detailed use and disclosure procedures.

4. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's or the City's own payment purposes, and PHI may be disclosed by a covered entity to a health care provider concerning the treatments of an individual for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication (e.g. claim administration) or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance), and related health care data processing.

Health Care Operations. PHI may be disclosed for purposes of the Plan's or the City's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Health care operations means any of the following activities to the extent that they are related to Plan administration.

- assist plan participants in claim resolution;

- determination of eligibility, coverage and cost sharing amounts (for example, cost sharing of a benefit, plan maximums and co-payments as determined for an individual's claim);
- coordination of benefits;
- subrogation of health benefit claims;
- population-based activities relating to improving health or reducing health care costs;
- 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 health care claims (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 Plan, including formulary development and administration, development or improvement of payment methods or coverage policies;
- business management and general administrative activities of the Plan, including, but not limited to:
 - (a) management activities relating to the implementation of and compliance with HIPAA's administrative simplification requirements, or
 - (b) customer service, including the provision of data analyses for resolution of internal grievances.

5. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the City's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

6. Mandatory Disclosures of PHI: to Individual and DHHS

A participant's PHI must be disclosed as required by HIPAA in two situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows); and
- The disclosure is made to the (DHHS) for purposes of enforcing of HIPAA.

7. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The City's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may

be made. The requirements may include prior approval of the City's Privacy Official. Permitted disclosures are:

- about victims of abuse;
- neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities, for health oversight activities;
- about decedents;
- for cadaveric organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions, and
- that relate to workers' compensation programs.

8. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

9. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

- For each of the following recurring disclosures:
benefit enrollment /changes, audits, claim resolution, obtaining identification cards, and responding to legal requests, the identifiers will be as follows: social security, medical records, account and health plan beneficiary numbers, names, geographic units, dates, ages over 89, phone/fax numbers, email addresses and any other unique identifiers. The persons who may receive the PHI will be account representatives, claims adjusters, attorneys, nurses, physicians, managers, supervisors, auditors, underwriters, insurance brokers, and the Human Resource Manager. The conditions will be as follows:
- determination of eligibility, coverage and cost sharing amounts (for example, cost of a benefit, plan maximums and co-payments as determined for an individuals claim);
- coordination of benefits;
- adjudication of health benefit claims (including appeals and other payment disputes);
- subrogation of health benefit claims;
- establishing employee contributions;

- risk adjusting amounts due based on enrollee health status and demographic characteristics;
- billing, collection activities and related health care data processing;
- claims management and related health care data processing, including auditing payments, investigating and resolving payment disputes, and responding to participant inquiries about payments;
- obtaining payment under a contract for reinsurance (including stop-loss and excess of loss insurance);
- medical necessity reviews or reviews of appropriateness of care justification of charges;
- utilization review, including pre-certification, preauthorization, concurrent review and retrospective review;
- disclosure to consumer reporting agencies related to the collection of premiums or reimbursement (the following PHI may be disclosed for payment purposes; name and address, date of birth, Social Security number, payment history, account number, and name and address of the provider and/or health plan).
- In the event of a power outage, the City's Electric Department needs to identify special needs of City customers who must utilize specialized equipment or medical equipment that requires electricity to remain on and will be limited to the minimum necessary for the purpose.
- In emergency situations in order for the Fire Department to perform or assist with emergency medical treatment it will be limited to minimum necessary for the purpose.
- In order for the Police Department to facilitate the necessary law enforcement process as it relates to arrestees and or suspects it will be limited to minimum necessary for the purpose.
- In order to determine eligibility for programs offered through the City's Housing Rehabilitation it will be limited to the minimum necessary for the purpose.

All other disclosures must be reviewed by the Privacy Official on an individual basis to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When the City is Requesting PHI. For making *requests* for disclosure of PHI the following applies:

- For claim payment, strategic planning with respect to the Plan, COBRA rate or funding level determination, information requested from the third party administrator and/or the Plan should be limited to summary health information or de-identified information to the extent possible. PHI should be requested only to the extent reasonably necessary to carry out these functions.
- To assist with claim and/or physician billing issues, requests for information from the third party administrator, health care providers and/or Plan should be limited to summary health information or de-identified information to the extent possible. PHI should be requested only to the extent reasonably necessary to assist individuals with resolution of their claims and/or physician billing issues.

- For claims audits, requests for information from the third party administrator and/or Plan should be limited to summary health information or de-identified information to the extent possible. PHI should be requested only to the extent reasonably necessary to carry out these functions.
- For Plan marketing, renewal, underwriting and experience evaluation, requests for information from the third party administrator and / or Plan should be limited to summary health information or de-identified information to the extent possible. PHI should be requested only to the extent reasonably necessary to carry out these functions.
- Requests for PHI from physicians and other health care providers for the purposes of providing day care and community services for the elderly and running the City's Early Learning Program shall be limited to the minimum information necessary to operate these programs and to maintain appropriate licensure.
- In the event of a power outage, the City's Electric Department needs to identify special needs of City customers who must utilize specialized equipment or medical equipment that requires electricity to remain on and will be limited to the minimum necessary for the purpose.
- In emergency situations in order for the Fire Department to perform or assist with emergency medical treatment it will be limited to minimum necessary for the purpose.
- To order for the Police Department to facilitate the necessary law enforcement process as it relates to arrestees and or suspects it will be limited to minimum necessary for the purpose.
- In order to determine eligibility for programs offered through the City's Housing Rehabilitation it will be limited to the minimum necessary for the purpose.

All other requests must be reviewed on an individual basis to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the DOL;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making *disclosures* of PHI to the medical plan, prescription plan, Employee Assistance Plan, dental plan, vision plan, reciprocal benefits plan, auditors, and attorneys for purposes of benefit enrollment/changes, audits, claim resolution, obtaining identifications cards, benefit eligibility, hospital reports on suspects/arrestees, and response to legal requests, by only giving information necessary to initiate the function.

All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from the prescription plan, Employee Assistance Plan, dental plan, vision plan, reciprocal benefits plan, auditors, and attorneys for purposes of benefit enrollment/changes, audits, claim resolution, obtaining identifications cards, benefit eligibility hospital reports on suspects/arrestees, and response to legal requests, by only giving information necessary to initiate the function.

All other requests must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

10. Disclosures of PHI to Business Associates

Employees may disclose PHI to the Plan's or the City's businesses associates and allow the Plans or the City's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan or the City, as applicable, must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing functions or activities for or on behalf of a covered entity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

11. Disclosures of De-Identified Information

The Plan or the City may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

Policies on Individual Rights

1. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan or the City, as applicable (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the City that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan, or
- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

2. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment, or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

The Plan or the City shall respond to an accounting request within 60 days. If the Plan or the City is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

3. Requests for Alternative Communication Means or Locations

Individuals may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the City, the requests are reasonable.

However, the City shall accommodate such a request if the individual clearly provides information that the disclosure of all or part of that information could endanger the individual. The Privacy Official has responsibility for administering requests for confidential communications.

4. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the City's policy to attempt to honor such requests if, in the sole discretion of the City, the requests are reasonable. The City of Lakeland's Privacy Official at the Office of Risk Management, is charged with responsibility for administering requests for restrictions.

Use and Disclosure Procedures

1. Procedures for Use and Disclosure of PHI

Procedure

Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations. An employee may use and disclose PHI to perform the Plan's or the City's own payment activities or health care operations.

- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Disclosures for Another Entity's Payment Activities. An employee may disclose a Plan participant's PHI to another covered entity or health care provider to perform the other entity's payment activities. Disclosures may be made under the following procedures:

- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Disclosures for Certain Health Care Operations of the Receiving Entity. An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are subject to the following:

- Disclosures must comply with the "Minimum-Necessary Standard."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, an employee may not use a participant's PHI for the payment or operations of the City's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow these steps:

- Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. *Employees shall not attempt to draft*

authorization forms. All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Official.

- Disclosures must comply with the "Minimum-Necessary Standard."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official.

2. Mandatory Disclosures of PHI: to Individuals and DHHS

Procedure

- **Request From Individual.** Upon receiving a request from an individual (or an individual representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."
- **Request From DHHS.** Upon receiving a request from a DHHS official for disclosure of PHI, the employee must take the following steps:
 - Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."
 - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

3. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

Procedure

- **Disclosures for Legal or Public Policy Purposes.** An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made under the following procedures:
 - The disclosure must be approved by the Privacy Official.
 - Disclosures must comply with the "Minimum-Necessary Standard."
 - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Legal and Public Policy Disclosures Covered

A. Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

- The individual agrees with the disclosure; or
- The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

B. For Judicial and Administrative Proceedings, in response to:

- An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order): and
- A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

C. To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:

- Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
- Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
- Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.
- Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
- Information that constitutes evidence of criminal conduct that occurred on the City's premises.

D. To Appropriate Public Health Authorities for Public Health Activities.

E. To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

F. To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

G. For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

H. **For Certain Limited Research Purposes**, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

I. **To Avert a Serious Threat to Health or Safety**, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

J. **For Specialized Government Functions**, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.

K. **For Workers' Compensation Programs**, only to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

4. Disclosures of PHI Pursuant to an Authorization

Procedure

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Verify that the authorization form is valid. Valid authorization forms are those that:
 - Are properly signed and dated by the individual or the individual's representative;
 - Are not expired or revoked. The expiration date of the authorization form must be a specific date (such as July 1, 2003) or a specific time period (e.g., one year from the date of signature), or to such time that employment with the City of Lakeland terminates;
 - Contain a description of the information to be used or disclosed;
 - Contain the name of the entity or person authorized to use or disclose the PHI;
 - Contain the name of the recipient of the PHI ;
 - Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
 - Contain a statement regarding the possibility for a subsequent re-disclosure of the information;
 - All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization;
 - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

5. Disclosure of PHI to Business Associates

Definition of Business Associate

Business Associate is an entity or person who:

- performs or assists in performing a function or activity for or on behalf of a covered entity involving the use and disclosure of PHI (including claims processing or administration including claim review assistance; data analysis, underwriting, including vendor selection processes, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the business associate access to PHI.

Procedure

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a "business associate" must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees must contact the Privacy Official and verify that a business associate contract is in place. The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the business associate contract.
- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum-necessary requirement, and each non-recurring disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

6. Requests for Disclosure of PHI From Spouse, Family Member or Friend

The Plan and City will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend will be able to access PHI.

- If an employee receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child, or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."
- Once the identity of a parent or personal representative is verified, then follow the procedure for "Individual's Request for Access."

- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

7. Disclosures of De-Identified Information

De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers as outlined in HIPAA regulations. The following identifiers must be removed to de-identify information:

- names
- all geographic subdivisions smaller than a state (special rules apply)
- all elements of dates (except year) relating to an individual (special rules apply)
- telephone numbers
- fax numbers
- electronic mail addresses
- Social Security numbers
- medical record numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identification and serial numbers including license plate numbers
- device identifiers and serial numbers (such as pacemaker number)
- web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- biometric identifiers including finger and voice prints
- full face photographic images and any comparable images, and
- any other unique identifying number, characteristic or code (special rules apply).

Procedure

- Obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.
- The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

8. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person

is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:

- Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.
- Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
- Make a copy of the identification provided by the individual and file it with the individual's designated record set.
- If the individual requests PHI over the telephone, their social security number will be requested as a means of identification.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:

- Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. [Insert information about relevant state law; in some circumstances, access by a parent may be denied if state law forbids access.]
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, the following steps should be followed:

- Require a copy of appropriate documentation such as a valid power of attorney [or other documentation-requirements may vary state-by-state]. If there are any questions about the validity of this document, seek review by the Privacy Official.
- Make a copy of the documentation provided and file it with the individual's designated record set.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI" the following steps should be followed to verify the official's identity and authority).

- If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
- If the request is in writing, verify that the request is on the appropriate government letterhead.
- If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Office of the City Attorney.
- Obtain approval for the disclosure from the Privacy Official.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

9. Complying With the "Minimum-Necessary" Standard

Procedures for Disclosures of PHI

- The standards for disclosures will be in accordance with policies on use of disclosure as referenced in the City of Lakeland HIPAA Privacy Disclosure Policy and Procedures.
- The amount of information requested will be the minimum amount to initiate the function.
- For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Procedures for Requests of PHI

- Recurring requests such as benefit enrollment/changes, audits, claim resolutions, obtaining identification cards, benefit eligibility and response to legal requests will follow as:

Telephone Requests – Steps to Follow

- Determine if Requestor is “known.”
- If unknown, tell Requestor to send written request on letterhead.
- Enter request into Disclosure of PHI logbook.
- If not for treatment, payment or health care operations (TPO), determine if there is a patient/client authorization.

Fax or Mail Requests – Steps to Follow

- Determine origin of request – check for seal or logo.
- If known, follow the same steps as for Telephone Request.
- If unknown, give the request to the Privacy Official to handle.

Requests Made in Person – Steps to Follow

- Verify the identity of the requestor with picture ID.
- If you are not certain give to the Privacy Official to handle.
- If requestor/request are verified, then follow the steps for Fax or Mail Requests.
- Each request will be limited to the minimum amount to initiate the function.

- For all other requests for PHI, contact the Privacy Official, who will ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Exceptions

The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to an individual authorization;
- Disclosures made to DHHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

10. Documentation

Procedure

Documentation. Employees shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants;
- When a disclosure of PHI is made;
 - the date of the disclosure;
 - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - a brief description of the PHI disclosed;
 - a brief statement of the purpose of the disclosure; and
 - any other documentation required under these Use and Disclosure Procedures.
- Individual authorizations.

11. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, if you become aware of a disclosure of PHI, either by an employee of Plan or an outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, immediately contact the Privacy Official so that the appropriate steps to mitigate any potential harm to the individual can be taken.

Procedures for Complying With Individual Rights

1. Individual's Request for Access

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the City that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a written request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. ***No request for access may be denied without approval from the Privacy Official.***
- Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, certain requests by inmates, information compiled during research when the individual has agreed to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. ***See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.***
- Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30- or 60-day period of the reasons for the extension and the date by which the City will respond.
- A Denial Notice must contain (1) the basis for the denial, (2) a statement of the individual's right to request a review of the denial, if applicable, and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.

- Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
- Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals also have the right to come in and inspect the information.
- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

2. Individual's Request for Amendment

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a written request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. ***No request for amendment may be denied without approval from the Privacy Official.***
- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above on PAGE 28). See the Privacy Official if there is any question about whether one of these exceptions applies. ***No request for amendment may be denied without approval from the Privacy Official.***
- Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the designated record set is accurate and complete without the amendment.
- Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the City will respond.
- When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed

on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.

- When an amendment request is denied, the following procedures apply:
 - All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
 - If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the City's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

3. Processing Requests for an Accounting of Disclosures of PHI

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, a written notice will be sent to the individual informing him or her that a fee for processing will be charged which will provide the individual with a chance to withdraw the request. The fee for processing will be as follows: Fifteen (15) cents per page. Also if extensive clerical or supervisory assistance by personnel of the City of Lakeland is involved, or both, the City of Lakeland may charge in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the cost incurred.

- Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below-). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the City will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to April 14, 2003.) The accounting does not have to include disclosures made:
 - to carry out treatment, payment and health care operations;
 - to the individual about his or her own PHI;
 - incident to an otherwise permitted use or disclosure;
 - pursuant to an individual authorization;
 - for specific national security or intelligence purposes;
 - to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
 - as part of a limited data set.
- If any business associate of the Plan has the authority to disclose the individual's PHI, then in order to obtain an accounting of the business associate's disclosures, the Privacy Officer for the plan will provide to the individual upon request the business associate's primary contact's name and telephone numbers:
- The accounting must include the following information for each reportable disclosure of the individual's PHI:
 - the date of disclosure;
 - the name (and if known, the address) of the entity or person to whom the information was disclosed;
 - a brief description of the PHI disclosed; and
 - a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
- If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official for more guidance.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements."

4. Processing Requests for Confidential Communications

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a written request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All confidential communication requests that are approved must be recorded in a written log that is maintained by the designated Privacy Official.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements:"

5. Processing Requests for Restrictions on Uses and Disclosures of PHI

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a written request from an individual (or a minor's parent or an individual's personal representative) to restrict access to an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- The employee should take steps to honor requests if disclosure could endanger the individual.
- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All requests for limitations on use or disclosure of PHI that are approved must be recorded in a written log that is maintained by the designated Privacy Official.
- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions which will be provided via written correspondence from the Privacy Official.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

Procedures to Safeguard PHI

Physical Security. Physical security of PHI will be maintained through various means as follows:

- PHI is to be maintained in separate file area of the office or enclosed room where access is limited to those City employees who have access according to the terms of the Privacy Policy. File cabinets should have locks. To the extent feasible, file cabinets should be kept locked.
- If PHI is stored in a desk, the desk should have a lock. Desks containing PHI should be locked when unattended. PHI is not to be left unattended on desktops, countertops or worktables.
- Departments that maintain PHI should ensure that visitors to the office are escorted to their contact person and not left unattended.
- Incoming mail should be delivered unopened to the person to whom it is addressed.
- If an employee receives PHI and the employee is not designated as being permitted to have access to PHI, the employee should redirect the PHI as soon as possible to an appropriate person who does have access to PHI.
- Fax machines should be kept in an enclosed area or room to limit access to incoming communications that may contain PHI. Employees should exercise reasonable care to keep incoming fax messages secure and limit access by other City employees.
- Address outgoing mail and fax communications only to the specific person at the organization who the organization has confirmed has access to PHI. Send PHI to a secure fax number verified by the intended receiver. Mark outgoing mail containing PHI “Personal & Confidential.”

Verbal Security.

- Employees shall take reasonable steps in verbally discussing PHI to ensure that PHI is not discussed with any employee, individual or third party who does not have access to PHI pursuant to the terms of the City’s Privacy Policy.
- PHI should not be discussed on speakerphone, unless necessary. If a speakerphone is used while discussing PHI, the door to the employee’s office should be kept closed.
- When discussing PHI by telephone, employees should take reasonable care that the party to whom they are speaking is permitted to have access to PHI.
- Employees should not discuss PHI in public areas such as elevators and lunch rooms or at social gatherings.

Supervisors should monitor physical and verbal security and access to PHI. Employees must report any violations of security to the Privacy Official as soon as possible.

Destruction of PHI.

- Discarded PHI should be left completely inaccessible.
- Do not use ordinary trash to discard PHI in any form (hard copy, diskette, CD, etc.)
- Paper documents containing PHI should be shredded whenever possible.

Electronic Security. Procedures for electronic security shall be determined on or before the HIPAA Security effective date of April 21, 2005.