CITY OF ST. PETERSBURG GROUP INSURANCE PROGRAM

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (‘HIPAA’)

PRIVACY POLICY AND PROCEDURES

Revised January 2019
# Table of Contents

Introduction ............................................................................................................. Page 4

**Privacy Policy and Procedures** ................................................................. Page
1. Privacy Officer and Contact Person .................................................................................. 5
2. Workforce and Disclosure to Plan Sponsor ......................................................................... 5
3. Technical and Physical Safeguards and Firewall .................................................................. 6
4. Privacy Notice ..................................................................................................................... 6
5. Complaints .......................................................................................................................... 7
6. Sanctions for Violations of Privacy Policy ........................................................................... 7
7. Mitigation of Inadvertent Disclosures of Protected Health Information .............................. 7
8. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy ................................. 8
9. Plan Document .................................................................................................................. 8
10. Documentation Requirements ............................................................................................. 9
11. Use and Disclosure of PHI ................................................................................................ 9
12. Mandatory Disclosures of PHI: to Individual and DHHS ................................................. 10
13. Permissive Disclosures of PHI: for Legal and Public Policy Purposes ............................ 10
14. Disclosures of PHI Pursuant to an Authorization ............................................................... 12
15. Disclosures of PHI to Business Associates ...................................................................... 13
16. Requests for Disclosure of PHI from Spouse, Family Member or a Friend .................... 13
17. Disclosures of De-Identified Information .......................................................................... 14

**Procedures for Reporting Violations** ............................................................ 15
1. Notification of Privacy Officer ............................................................................................. 15
2. Violation Resolution ........................................................................................................... 15
3. Violation Tracking ............................................................................................................... 15
Procedures for Complying with Individual Rights ........................................... 15

1. Access to Protected Health Information and Requests for Amendment .................... 15
2. Accounting ........................................................................................................... 18
3. Requests for Alternative Communication Means or Locations .................................. 20
4. Processing Requests for Confidential Communications ............................................. 20
5. Requests for Restrictions on Uses and Disclosures of PHI ........................................ 21

Procedures for Verification of Identity ........................................................................ 22
City of St. Petersburg
Group Insurance Program
HIPAA Privacy Policy and Procedures

Introduction

The City of St. Petersburg Group Insurance Program (‘Plan’) is a group plan, including medical, dental, vision, Flexible Spending Accounts (‘FSA’), Health Reimbursement Accounts (‘HRA’) and the Employee Assistance Plan (‘EAP’) sponsored by the City of St. Petersburg (‘City’). Members of the City of St. Petersburg’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 of St. Petersburg, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations restrict the ability to use and disclose Protected Health Information* (“PHI”). The Plan and the City intend to comply with the HIPAA Privacy Rules, to the extent its requirements are applicable to the Plan.

To that end, all members of the City of St. Petersburg’s workforce who have access to PHI must comply with the Privacy Policy and Procedures. For purposes of this Policy and these Procedures, the City of St. Petersburg’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 of St. Petersburg, whether they are paid by the City of St. Petersburg. The term "employee" includes all 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 these Procedures. The Plan reserves the right to amend or change these Procedures at any time (and even retroactively) without notice. To the extent these Procedures establish requirements and obligations above and beyond those required by HIPAA, the Procedures shall be inspirational and shall not be binding upon the Plan or the Employer. These Procedures do not address requirements under other federal laws or under state laws.

*Protected Health Information. Protected health information means information that is created or received by the Plan or the City 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.
1. Privacy Officer and Contact Person

The Privacy Officer will be responsible for 1) the development and implementation of policies and procedures relating to privacy, including, but not limited to these Privacy Procedures; and 2) the development and maintenance of a Notice of Privacy Practices. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer is responsible for ensuring that the Plan complies with all applicable requirements of the HIPAA Privacy Rules, including the use and disclosure rules and individual rights requirements. The Privacy Officer will monitor the agreement in place with each Business Associate*. The Privacy Officer will work with the Plan’s Security Officer with respect to electronic PHI. The Plan’s Privacy Officer is:

Vicki A. Grant, CBP, PHR  
Manager, Benefits  
City of St. Petersburg

*Business Associate – An entity that 1) creates, receives, maintains or transmits PHI on behalf of a covered entity (a health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction) including for claims processing or administration, data analysis and/or underwriting; 2) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation or financial services to a covered entity, where the performance of those services involves access to PHI; or 3) includes any sub-contractors of Business Associates who directly contract with the Plan or the City of St. Petersburg.

2. Workforce and Disclosure to Plan Sponsor

All members of the City of St. Petersburg’s workforce (described at the beginning of these Procedures and referred to herein as "employees") must comply with the City of St. Petersburg privacy policy and its use and disclosure procedures, which are set forth in this document and in the procedures adopted by affected departments and/or locations.

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

Each workforce member with access to PHI will receive HIPAA training within a reasonable period after joining the workforce. Training for all workforce members will occur within a reasonable time after a material change in the Plan’s Policy and Procedures.
The Plan may disclose PHI to the City for plan administration functions. Workforce members with access to PHI may not disclose PHI to other workforce members unless the disclosure is made pursuant to an individual’s valid HIPAA authorization or the disclosure has been approved by the Privacy Officer.

Workforce members with access to PHI must take all appropriate steps to ensure that PHI is not used or disclosed for employment purposes or in connection with another benefit or benefit plan maintained by the City. PHI that is disclosed to the City may not be used for employment purposes or in connection with another benefit or benefit plan maintained by the City, unless authorized by the individual pursuant to a valid HIPAA authorization.

3. Technical and Physical Safeguards and Firewall

The City of St. Petersburg will establish 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 (‘minimum-necessary standard’*) for plan administrative and healthcare provider functions, and that the employee will not further use or disclose PHI in violation of HIPAA’s privacy rules.

*Minimum Necessary Standard - When using or disclosing PHI, the Plan will make a reasonable effort to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The standard does not apply to 1) uses and disclosures made to the individual who is the subject of PHI; 2) Uses or disclosures made pursuant to a valid HIPAA authorization; 3) Disclosures made to DHHS; 4) Uses or disclosures that are required by law; and 5) Uses and disclosures that are required to comply with HIPAA. The Privacy Officer will implement procedures for limiting the disclosure of PHI and for requesting of PHI from another covered entity to the amount reasonably necessary to achieve the purpose of the disclosure (for routine and recurring requests as well as individual requests).

Complete details can be found in the Plan’s ‘HIPAA Security Policies and Procedures Manual’.

4. Privacy Notice

The Privacy Officer 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 or by The City of St. Petersburg;
- Individual's rights;
• The Plan’s legal duties with respect to PHI;
• Other information required by the HIPAA Privacy Rule.

The privacy notice will inform participants that the Plan will have access to PHI in connection with its administrative and healthcare functions. The privacy notice will also provide a description of the 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 and will be posted on the City’s intranet and internet websites:

• At the time of an individual’s enrollment in the Plan or upon request;
• Within 60 days after a material change to the notice;
• Not less frequently than once every three years.

5. Complaints

The Privacy Officer will be the Plan’s contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the 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. Complaints and reports of policy violations should be directed to:

Vicki A. Grant, CBP, PHR
Manager, Benefits
City of St. Petersburg
P. O. Box 2842
St. Petersburg, FL 33731-2842
(727) 893-7372
Vicki.Grant@stpete.org

6. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of the Plan’s HIPAA Privacy Policy and Procedures will be imposed in accordance with the City of St. Petersburg Rules and Regulations of the Personnel Management System.

7. Mitigation of Inadvertent Disclosures of Protected Health Information

The Plan 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 Privacy Policy and Procedures. As a result, if an employee becomes aware of a use or disclosure of protected health information, either by an employee of the City of St. Petersburg or an outside consultant/contractor or Business Associate, that is not in compliance with the Privacy Policies and Procedures the
employee should immediately contact the Privacy Officer 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

The Plan (and the City) may not intimidate, threaten, coerce, harass, discriminate against or take other retaliatory action against individuals for exercising their rights, filing a complaint or participating in any process provided under the HIPAA privacy rule, 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 Plan for administrative purposes. Specifically, the Plan document requires the Plan 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 of St. Petersburg;
- Not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Upon written request(s), make PHI available to Plan participants in accordance with the Privacy Rules requirements, consider their request for amendment to PHI and provide them with an accounting of PHI disclosures to the extent applicable and as required by law;
- Make the Plan’s internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (DHHS) upon request;
- 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.
- Ensure adequate separation between the Plan and the City, as required by the HIPAA Privacy Rule.

The Plan document also requires the City of St. Petersburg to (1) certify to the Privacy Officer that the Plan documents have been amended to include the above restrictions and that the City of St. Petersburg agrees to those restrictions; and (2) to provide adequate safeguards.
10. Documentation Requirements

The Plan’s Privacy Policy and Procedures shall be documented and maintained for at least six years from the date they were last in effect. The Policy 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) and any changes in the Plan’s operations or environment. Any changes to the policy or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy notice 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 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.

The Privacy Officer shall maintain copies of all 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/patients.
- 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. Use and Disclosure of PHI

The Plan may use and disclose PHI only as required or permitted under the HIPAA Privacy Rule and this Privacy Policy. The Plan may use and disclose PHI 1) For the Plan’s own payment and health care operations; 2) To another covered entity or health care provider for the payment activities of the receiving entity; 3) For the treatment activities of a health care provider; and 4) To another covered entity for purposes of that entity’s health care operations the entity has (or had) a relationship with the individual and the PHI pertains to that relationship, subject to the approval of the Privacy Officer.
12. 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;
- The disclosure is made to Department of Health and Human Services for purposes of enforcing of HIPAA.

Procedure

- **Request from Individual.** Upon receiving a written request from an individual (or an individual’s personal representative) for disclosure of the individual’s own PHI, the employee must follow the procedure for "Request from Individual, Parent of Minor Child or Personal Representative” under the "Access to Protected Health Information and Requests for Amendment" section of these procedures.

- **Request From DHHS.** Upon receiving a request from a Department of Health and Human Services (“DHHS”) Officer for disclosure of PHI, the employee must take the following steps:
  - Follow the procedures for verifying the identity of a public Officer set forth in "Verification of Identity of Those Requesting Protected Health Information."
  - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

13. Permissive Disclosures of PHI: for Legal and 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 Officer. Disclosures may be made under the following procedures:

- The disclosure must be approved by the Privacy Officer.
- 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

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Plan’s use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan’s Privacy Officer.

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 Officer 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; or
• Information that constitutes evidence of criminal conduct that occurred on the City of St. Petersburg 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 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 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 Officers 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.

14. 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 individual (or his or her personal representative). All uses and disclosures made pursuant to the receipt of a signed ‘Authorization for Use and/or Disclosure of Protected Health Information’ form must be consistent with the terms and conditions of the 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 the Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the employee must:

- Follow the procedures for verifying the identity of the individual (or individual's personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information";
- Verify that the completed ‘Authorization Form’ form is valid. Valid forms are those that:
  - Are properly signed and dated by the individual or the individual's personal representative;
  - Are not expired or revoked. (The individual will specify the expiration date of the authorization on the completed ‘Authorization for Use and/or Disclosure of Protected Health Information’ form);
  - 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;
• 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."

15. Disclosures of PHI to Business Associates

The Plan may disclose PHI to a Business Associate, and may allow a Business Associate to create, receive, maintain or transmit PHI on its behalf. However, prior to doing so, the Plan 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 Officer 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 standard, and each non-recurring disclosure must be approved by the Privacy Officer.)
• Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

16. Requests for Disclosure of PHI from Spouse, Family Member, Friend or Personal Representative

The Plan and The City of St. Petersburg 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, friend or personal representative 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, the employee must 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 Authorization."

17. Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information in accordance with the HIPAA Privacy Rule. 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

- The employee must obtain approval from Privacy Officer for the disclosure. The Privacy Officer will verify that the information is de-identified.
- The Plan may freely use and disclose de-identified information. De-identified information is not PHI.
PROCEDURES FOR REPORTING VIOLATIONS

1. Notification of Privacy Officer

   • Any employee who believes that a violation of the Privacy Policy has occurred is required to contact the Privacy Officer immediately to report the incident in question. The ‘Report of Violation’ form should be used to document and report a suspected violation.
   • The Privacy Officer will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action.

2. Violation Resolution

   • The Privacy Officer will notify all involved parties, such as affected employee(s), the Plan, the City of St. Petersburg, and the third-party service provider, in a timely manner once it has been determined that a violation of the Privacy Policy has occurred.
   • The resolution of such violation will seek to restore the level of privacy that is required under this Policy.
   • The Privacy Officer will correct any deficiency in the Privacy Policy or related procedures that contributed to the violation.
   • Employee(s) found responsible for the violation will be subject to disciplinary action in accordance with the City of St. Petersburg Rules and Regulations of the Personnel Management System. The Privacy Officer and the City of St. Petersburg will make this determination.
   • If a violation is found to have occurred due to the actions of a third-party service provider, the Privacy Officer and the City of St. Petersburg will take appropriate action up to and including terminating the service provider’s relationship.

3. Violation Tracking

   The Privacy Officer will maintain relevant information on all reported incidents of potential violation under this Policy whether or not a reported incident is ultimately found to be an actual violation. The Privacy Officer will track reported violations.

PROCEDURES FOR COMPLYING WITH INDIVIDUAL RIGHTS

1. Access to Protected Health Information and Requests for Amendment

   HIPAA gives individuals the right to access and obtain copies of their PHI that the Plan or City of St. Petersburg (or their Business Associates) maintain in ‘designated record sets’*. HIPAA also provides that individuals may request to have their PHI amended.
The City of St. Petersburg will provide access to PHI that are submitted by individuals completing the ‘Record Access Request Form’ and it will consider requests for amendment that are submitted by individuals by completing the form ‘Request to Amend Protected Records’.

*Designated Record Set* is a group of records maintained by or for The City of St. Petersburg that includes:

- The medical and billing records about individuals maintained by or for a covered healthcare provider;
- 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 the Plan to make decisions about an individual.

**Procedure:**
**Request from Individual, Parent of Minor Child, or Personal Representative.** Upon receiving a completed ‘Authorization for Use and/or Disclosure of Protected Health Information’ form 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 Officer if it appears that the requested information is not held in the individual's designated record set;
- 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. The employee must see the Privacy Officer if there is any question about whether an exception applies. No request for access may be denied without approval from the Privacy Officer;
- 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 Plan 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 Officer.

- Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, the employee will 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 of the requested information by mail, e-mail, in another electronic format or by physically inspecting the information at the City of St. Petersburg Benefits Division office;
- 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."
- The Plan may impose a reasonable, cost-based fee for copies of requested PHI, provided that the fee may only include the cost of 1) labor for copying the PHI; 2) Supplies for creating the paper copy or electronic media; or 3) postage.

Procedure:
Request for Amendment from Individual, Parent of Minor Child, or Personal Representative. Upon receiving a completed ‘Request to Amend Records’ form 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 at issue is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record set;
- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access. The employee must see the Privacy Officer if there is any question about whether an exception applies. No request for access may be denied without approval from the Privacy Officer;
- 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 Plan 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 notice of denial must be approved by the Privacy Officer. 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 Plan'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.

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 a HIPAA 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;
- For other national security or indolence purposes;
- To correctional institutions or law enforcement officials.
The Plan shall respond to an accounting request within 60 days. If the Plan 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 Officer may impose reasonable cost-based fees for subsequent accountings.

Procedure:
Request from Individual, Parent of Minor Child, or Personal Representative. Upon receiving a completed ‘History of Non-Routine Disclosures Request Form’ 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";
- 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, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request;
- 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 Plan 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:
  1) To carry out treatment, payment and health care operations;
  2) To the individual about his or her own PHI;
  3) Incident to an otherwise permitted use or disclosure;
  4) Pursuant to an individual authorization;
  5) For specific national security or intelligence purposes;
  6) To correctional institutions or law enforcement when the disclosure was permitted without an authorization;
  7) As part of a limited data set.
• If any business associate of the Plan has the authority to disclose the individual's PHI, then the employee must issue a written request to the Privacy Officer of the business associate. Business associate contact information can be obtained by contacting the Privacy Officer, by written request.

• The accounting must include the following information for each reportable disclosure of the individual's PHI:
  1) the date of disclosure;
  2) the name (and if known, the address) of the entity or person to whom the information was disclosed;
  3) a brief description of the PHI disclosed; and
  4) 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 officer 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 Officer for more guidance.

• Accounting must be documented in accordance with the procedure for "Documentation Requirements."

3. Requests for Alternative Communication Means or Locations

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

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

4. Processing Requests for Alternate and/or Confidential Communications

Procedure

Request from Individual, Parent of Minor Child, or Personal Representative. Upon receiving a completed ‘Request for Alternate Communication’ form 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."; and
• 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.
• The employee should take steps to honor requests that the Plan believes can be reasonably accommodated. The Plan will honor requests for alternative communication means or location if such a request provides clear information that a participant could be endangered if the request for alternative communication means or location is not granted. 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 approved, in writing, by the Privacy Officer.
• Requests and their dispositions must be documented in accordance with the procedure for “Documentation Requirements”.

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

An individual may request restrictions on the use and disclosure of the participant’s PHI. It is the Plan’s policy to attempt to honor such requests if, in the sole discretion of the Plan, the requests are reasonable. The Privacy Officer is charged with responsibility for administering requests for restrictions. If the request for restrictions is not reasonable, the Plan may deny the request by written notice to the participant.

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) 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 that can be reasonably accommodated. The employee should take steps to honor request for limitations on the use or disclosure of PHI if the denial of such request 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 approved, in writing, by the Privacy Officer.
• Notify all business associates that may have access to the individual's PHI of any restrictions that have been approved; and
• Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

PROCEDURES FOR
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.

Procedure
Request Made by Individual. When an individual requests access to his or her own PHI, the employee must:
  • 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 Officer.
  • Make a copy of the identification provided by the individual and file it with the individual's designated record set.
  • Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Procedure
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.
  • 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.
- If there are questions about the validity of this document, seek review by the Privacy Officer.
- 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."

Procedure

Request Made by Public Officer. If a public officer 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 Officer's identity and authority:

- If the request is made in person, request presentation of an agency identification badge, other officer 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 Legal Department, City of St. Petersburg.
- Obtain approval for the disclosure from the Privacy Officer.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."