Port of Seattle HIPAA Privacy Policy
February 2019

Policy Statement: The Port of Seattle offers various group health and benefit plans to Port employees and retirees. The Port of Seattle is a hybrid entity as defined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Port of Seattle's group health plan(s) is designated as the health care component of the Port of Seattle (the Port). Both the group health plan and the Port employees whose work it is to administer the Port's group health plans, shall comply with the requirements of the Administrative Simplification requirements of the HIPAA Privacy, Security and Breach Notification Rule as set forth in Title 45, Parts 160, 162 and 164 of the Code of Federal Regulations (the "CFR").

Purpose: This policy describes how Protected Health Information can be used and disclosed under the HIPAA Privacy Rule. It defines the rights of Plan Members with regards to their Protected Health Information that is created, received, maintained transmitted and/or stored by the Port. It defines organization safeguards that the Port is required to maintain. The Privacy Officer has sole responsibility, with support from others as appropriate, for implementing this policy and any related procedures, in consultation with the Legal Department. All references to the Privacy Officer shall mean the Benefits Manager. Uses and disclosures of Protected Health Information by the Port's service providers shall be governed by applicable Business Associate Contracts.

Scope: This policy contains information on the following topics:

- Uses and Disclosures of Protected Health Information (PHI) that Can Always Be Made Without Permission
- Uses and Disclosures of PHI that Shall Be Made if Specific Conditions Are Met
- Uses and Disclosures of PHI that May Be Made if Specific Conditions Are Met
- Authorizations by a Plan Member to Release PHI
- Plan Member Rights
- Organizational Requirements
- Breach Notification

1) Uses and Disclosures of Protected Health Information that Can Always Be Made Without Permission

Protected Health Information may be disclosed without participant or beneficiary permission for certain purposes, provided the requirements of this policy, these procedures and the HIPAA Privacy Rule are met. Any use or disclosure of Protected Health Information not outlined below or otherwise required by law shall be made pursuant to a written authorization of the plan participant, as set forth in the HIPAA Privacy Rule.

a) All uses and disclosures of Protected Health Information for payment activities shall be limited to the minimum amount of information necessary to carry out the intended purpose, to the extent such limitation is imposed by the HIPAA Privacy Rule. The following uses and disclosures of Protected Health Information for "payment" purposes are permitted:

   i) Payment of medical and dental claims invoices.

   ii) Payment of LEOFF-1 retiree claims reimbursement requests, including review by the King County LEOFF-1 Disability Board.

   iii) Payment of retiree and COBRA premiums.

   iv) Payment of flexible spending account reimbursement invoices.

   v) Assist group health plan members with payment and claims issues

   vi) Additional uses and disclosures may also fall within the HIPAA Privacy Rule's definition of "payment." The Privacy Officer will determine on a case-by-case basis if a particular use or disclosure not listed above is a payment activity. If that activity is common or recurring, it shall be added to the list above.

b) The following uses and disclosures of the Port's Protected Health Information for "health care operations" purposes are permitted:

   i) Accessing vendor web portals to review and update medical, dental, wellness, health savings accounts, and healthcare flexible spending account information and reports.

   ii) Receiving and sending verbal, electronic and hard-copy reports and emails on medical, dental, wellness, health savings account, and flexible spending account activity.

   iii) Analyzing and planning benefits program design.

   iv) Providing enrollment and medical data to subrogation vendor

   v) Responding to child support order information requests

vi) Providing medical information and data to Employee Relations staff as required to implement other Federal laws

vii) For the health care operations activities of another covered entity. Upon request by another covered entity, the Port will disclose Protected Health Information for purposes of the requestor's health care operations activities if the following conditions are met:

(1) The other entity has or had a relationship with the participant or beneficiary who is the subject of the Protected Health Information.

(2) The other entity certifies to the Port that the disclosure is necessary for the other entity to perform health care operations activities, such as:
(a) Payment coordination, such as allowing web portal access to ensure proper payment of retiree premiums.
(b) Case management, such as sharing verbal, electronic and hard-copy reports and emails on medical and dental account activity
(c) Health care fraud and abuse detection or compliance.

(3) The Port will make a good faith effort to determine that the information requested by a covered entity is the minimum necessary.

viii) Additional uses and disclosures may also fall within the HIPAA Privacy Rule's definition of "health care operations." The Privacy Officer will determine on a case-by-case basis if a particular use or disclosure not listed above is a health care operations activity. If that activity is common or recurring, it shall be added to the list above.

2) Uses and Disclosures of Protected Health Information that Shall Be Made if Specific Conditions Are Met

a) Releases of Information to Friends and Family. The Port may disclose, without an authorization, to persons involved in the care of a plan member such as a family member, relative, close personal friend or other persons identified by the plan member, general condition or PHI directly related to the person's involvement in the plan member's care (including payment of the plan member's care) in the circumstances explained below. The Port shall always attempt to provide the plan member with the option to object to such release verbally prior to disclosure.

i) If the plan member cannot agree or object to the disclosure (because the plan member is not present, or due to incapacity or emergency), workforce members may exercise professional judgment to determine whether the disclosure is in the plan member's best interests and if so, disclose limited

general information about the plan member's PHI directly relevant to the extent of person's involvement with the plan member's care.

ii) If the Port receives a request for PHI from a plan member's family, relative, or close friend, who is actively involved in the care of the plan member, workforce members shall attempt to allow the plan member the opportunity to object to the release of PHI. Such objection does not need to be in writing but does need to be noted in the plan member's record.

iii) If the plan member does not object or is not in a position to object, The Port's workforce shall use professional discretion and release PHI appropriate to the situation. If no objection is made regarding the disclosure, PHI may be disclosed to the family member or friend. This shall also be documented in the plan member's record.

iv) If the plan member objects to release of information to the individual requesting access to PHI, including health condition, PHI shall not be disclosed unless, in the professional judgment of the workforce member, the individual is critical to the care of the plan member and the need to know is appropriate.

b) Release for Judicial and Administrative Proceedings. The Port will release PHI for judicial and administrative proceedings upon receipt of court documents specifically authorizing such release. Release will also be made pursuant to a duly authorized subpoena. The Port will ascertain that the individual whose PHI is to be released has been properly notified about the subpoena prior to PHI release.

i) Court Order or Governmental Administrative Request.

(1) When the Port receives a court order or governmental administrative request for a plan member's PHI, the request will be authenticated before any PHI is released.

(2) Refer the request for disclosure to the Legal Department which will determine the validity of the request, in consultation with the Privacy Officer.

(3) If the court order or request is deemed valid, the minimum amount of PHI necessary to satisfy the court order or request will be released to the court or governmental agency.

(4) Such release or denial of release shall be documented in the plan member record.

(5) The disclosure shall be included in the list of disclosures.

ii) Subpoena

(1) The preceding procedure will also be followed if a subpoena is received.

(2) All attorney subpoenas received requesting "any and all" plan member PHI will be referred to the Legal Department.

(3) The Legal Department or designee will contact the attorney and request clarification regarding the need for the PHI or the specific purpose behind the request. The Legal Department may also require the attorney to obtain a court order.

(4) The Port will not release PHI to the attorney until the organization receives a court order or revised subpoena specifically defining what PHI is needed and for what purpose.

(5) When appropriate documentation is received, the Legal Department will direct the Privacy Officer to release the appropriate PHI to satisfy the subpoena after the individual has been notified.

(6) Such release or denial of release shall be documented in the plan member record.

(7) The disclosure shall be included in the list of disclosures.

c) Releases to a Legal Representative. The Port shall release to a legal representative as defined by state law (also referred to as "personal representative") relevant PHI pursuant to a written authorization signed by the legal representative. The Port must treat a legal representative of a plan member, designated and authorized under state law, just as they would treat the plan member to the extent that PHI is relevant to the matters on which the legal representative is authorized to represent the plan member. This includes parents of minor children, court-appointed guardians, and persons with power of attorney. The Port will treat any person authorized to act as the personal representative of a participant or beneficiary that is deceased (*e.g.*, an executor or administrator) as though he or she is the participant or beneficiary.

i) **I**f the Port receives an authorization for release of PHI from a legal representative of a plan member, documentation such as a court order, specific power of attorney or healthcare power of attorney needs to accompany the authorization.

ii) If appropriate documentation does not accompany the request for PHI, the Port shall request such documentation.

iii) If appropriate documentation is not provided, release of PHI will be denied unless otherwise authorized under the HIPAA Privacy Rule.

iv) If received documentation is found to be satisfactory upon review, appropriate PHI will be released to the legal representative of the plan member.

v) If the documentation received is questionable, the authorization from the legal representative and documentation regarding the authority of the legal representative shall be forwarded to the Legal Department who is responsible for resolving and approving or disapproving what may be considered questionable documentation.

vi) Such release or denial of release shall be documented in the plan member record.

vii) The disclosure shall be included in the list of disclosures.

d) Workers' compensation. The Port will disclose Protected Health Information in compliance with applicable state and federal workers' compensation laws (*i.e.*, any state or federal law that has the effect of providing benefits for work-related injuries or illness without regard to fault). Workers compensation teams are specifically exempted from coverage under the Privacy Rule. Since the Port self-insures, the business activities of the Workers Compensation Team are specifically exempted from coverage under the HIPAA Privacy Rule. The minimum necessary requirement applies to any release of plan member PHI to the workers compensation team.

i) If a request for release of plan member PHI is received from the workers compensation team, the request will be reviewed to determine if such request is valid.

ii) If questions arise regarding the validity of the request, the request will be referred to the Privacy Officer who is responsible for request validation.

iii) If the request is deemed invalid, the Privacy Officer shall contact the workers compensation team and inform the team that the plan member PHI will not be released and specify the reason why the PHI will not be released.

iv) If the request is deemed valid, requested information shall be compiled and forwarded to the workers compensation team.

v) Any release made for workers compensation purposes shall include only the PHI necessary to meet the request.

vi) PHI generally will consist only of information specifically related to the injury or any pre-existing condition that may have contributed to the injury.

vii) Release of PHI allegedly related to a pre-existing condition that contributed or exacerbated the injury shall be reviewed by the Privacy Officer prior to inclusion in the release.

viii) If it is determined that pre-existing condition PHI is not related to the injury documented in the workers compensation claim, the workers compensation team shall be provided only PHI related to the injury.

ix) No plan member PHI that is specially protected by state or federal law shall be released to the workers compensation team without specific authorization from the plan member. This includes genetic, mental health, HIV/AIDS, sexually transmitted diseases, alcohol and chemical dependency, birth control and certain identifiable health information of minors.

x) The disclosure shall be included in the list of disclosures.

xi) Any information regarding the release shall be retained for a minimum of six years

3) **Uses and Disclosures of PHI that May Be Made if Specific Conditions Are Met**

a) Releases of Information to a Minor. Under most circumstances, the Port shall obtain written authorization from a parent, guardian, or person acting in the place of a parent to use and disclose protected health information (PHI) to a minor if the minor has not reached the age of 18. The parent (or guardian or other person acting in the place of a parent) is usually able to exercise rights and authorities on behalf of the minor except under certain conditions as defined in state law, which include

- Minor is legally emancipated
- Minor is married

- Minor has reached age of informed consent and is seeking diagnosis and treatment for
    - Alcohol and chemical dependency treatment – 13 or older
    - Mental health – 13 or older
    - Sexually transmitted diseases, including HIV – 14 or older
    - Birth control – no minimum age

i) A minor may consent to the use or disclosure of PHI and exercise exclusive rights with respect to such information if:

(1) The minor's parent assents to an agreement of confidentiality between the physician and the minor with respect to such health care service; or

(2) The minor lawfully obtains a health care service without the consent of or notification to a parent, guardian or other person acting in the place of the parent and the minor has not requested that such person be treated as the legal representative. In those instances where the Port must have the plan member or legal representative's written permission to use or disclose the minor's PHI, it must obtain the minor's written permission to use or disclose the PHI.

ii) If the Port receives a request for release of PHI from a minor plan member, the workforce member shall request parent or legal representative authorization prior to releasing information to the minor (see the document Providing Health Care to Minors Under Washington Law, Appendix A to this document, for exceptions).

(1) If the minor is of the age of consent under state law, PHI will be released to the minor without authorization from the parent or legal representative.

(2) If authorization is not received, the minor's request for release of PHI will be denied in writing. The denial will also become part of the minor's plan member file.

b) Public health activities. Uses or disclosures of Protected Health Information for public health activities will be rare. Contact the Privacy Officer for any uses or disclosures potentially falling within this category.

c) National security and intelligence activities.

i) The Privacy Officer shall authorize the disclosure of Protected Health Information to authorized federal officials for intelligence and other national security activities.

ii) Disclosures for national security and intelligence activities are not subject to

the disclosure accounting.

4) Authorization for Release of PHI.

The Port shall not release PHI to third parties for purposes other than treatment, payment and healthcare operations, or as otherwise allowed by law, without the specific authorization of the plan member or the plan member's authorized personal representative.

If the plan member requests that a copy or a summary of his or her designated record set be sent directly to a third person, the Port shall honor that request if it is received in writing, signed by the individual, and clearly identifies the designated person and where to send the copy of protected health information. Use of a more specific authorization form shall not be required.

The Port shall not release PHI specifically protected by state law or other federal law for any purpose without the specific authorization of the plan member or authorized personal representative. This includes PHI that discloses sexually transmitted diseases including HIV, genetic, mental health, and chemical dependency/alcohol abuse and birth control information.

Any authorization for release of information needs to specifically identify what is to be released in as great a detail as possible. All authorization forms also must be time limited (e.g., the authorization is valid until X date) or event driven (e.g., the authorization is valid until X occurs). The Port has adopted specific authorization forms for use when releasing PHI to a third party. The form includes check boxes to specifically authorize release of specially protected PHI.

a) Third Party Request for Release of Protected Health Information

   i) If the Port receives a request from a third party for release of PHI for other than treatment, payment, healthcare operations or as otherwise authorized by law the request will be routed to the Privacy Officer.

   ii) The Privacy Officer will review the request and consult with the Legal Department when needed to determine if specific authorization is required.

   iii) If specific authorization is required, the Privacy Officer will contact the plan member or authorized personal representative in writing explaining the nature of the request for release and send the appropriate authorization form with the letter. The communication will state that if authorization is granted by an authorized personal representative, the returned authorization form needs to be accompanied by appropriate documentation validating that the personal representative has the authority to represent the plan member.

iv) If authorization is granted, the Privacy Officer will notify the third party requesting the information that authorization has been granted and will include requested information with the letter.

v) If the plan member, or authorized personal representative denies release, the Privacy Officer will notify the third party requesting the information that authorization has been denied by the plan member or authorized personal representative. Notification will be in writing.

vi) All letters and signed acknowledgement forms shall become part of the plan member's record.

b) Authorization for Release to Port

i) The Port has adopted a specific authorization form for release of PHI by a third party to the Port.

ii) If the Port requires access to third party PHI for purposes other than treatment, payment, healthcare operations, as allowed by law or access to specifically protected PHI under state and federal law, the workforce member will first document the need and purpose for release.

iii) The appropriate authorization form will be mailed to the plan member or authorized personal representative specifying in as much detail as possible the PHI requested by the Port accompanied by a letter specifying the reason for the release of PHI.

iv) If authorization is granted and the PHI forwarded to the Port, the released PHI shall only be used for the purposes documented. The authorization form received from the plan member or authorized personal representative shall become part of the plan member's record.

v) If the authorization is required to seek payment for services rendered and the plan member refuses to sign the authorization form, the plan member will be directly billed for services.

vi) All letters and forms shall become part of the plan member's record.

5) Plan Member Rights.

The HIPAA Privacy Rule requires that covered entities provide plan members with a number of rights around their protected health information.

a) Notice of Privacy Practices. A Notice of Privacy Practices (NPP) will be given to any new plan member at the time of hire or enrollment. The Notice will clearly define how the Port will use and disclose a plan member's health information and plan member rights. The Notice will also include additional health information protections afforded by Washington state law and will clearly state the ways in which a plan member can exercise his/her rights.

   i) The Notice is a public document. The Port will provide the NPP upon request of any person. The requestor does not have to be a current plan member.

   ii) The Port will prominently post the Notice on the Port's website.

   iii) The Port has the right to change the Notice at any time. The revised privacy practices will not be implemented prior to the effective date of the revised notice. The Port will apply the revised practices to only that PHI is created or received under the revised notice.

   iv) The Port will retain copies of every version of the Notice issued for a minimum of six years.

b) Access to Designated Record Set. The HIPAA Privacy Rule grants plan members the right to request a copy or to view their plan record. With certain exceptions, plan members have a right to access (or to obtain a copy of), records pertaining to the plan member and any other PHI that the Port maintains if the information is used, in whole or in part, to make decisions about plan member payment. The request for records must be in writing and signed by the plan member, if the plan member is capable of giving consent, or otherwise by the plan member's legal representative or such other person authorized by law. The Port may charge the plan member for a copy of his or her record or for a summary of the plan member's record. The Port will not charge a plan member if the plan member requests the opportunity to view his or her record. Charges for copies are limited by state law and the plan member will be informed in advance of the cost of providing a copy of the full record or a summary of the record. The plan member is also entitled to an electronic copy of the plan member's record.

   i) Plan Member Request for Copy of Record:

(1) The Port shall inform plan members that requests for copies or summaries of records must be in writing.

(2) A form to be completed by the plan member requesting access to his or her record will be readily made available upon request.

(3) If any requests are made, the Port will store the written request for a period of no less than six years.

(4) The Port will designate a member of the workforce to process any requests for copies or summaries of a plan member record, or requests to view a plan member record.

(5) The Port will accept, deny or partially deny the written request for access within 30 days of receipt of the request.

(6) If the Port is unable to provide access to the record within this period, the period to compile the record can be extended no more than an additional 30 days.

(7) If such an extension is necessary, the plan member must be notified in writing of the reason for the delay and the expected date on which the record will be made available. This notification must occur within the initial 30-day period.

ii) Viewing the Record

(1) The Port cannot charge the plan member if the plan member requests to examine or view his or her record.

(2) If the plan member requests to view his or her record, the appropriate documents will be compiled and a mutually convenient time will be scheduled to allow the plan member the opportunity to view his or her record.

(3) If the Port denies access to any part of the plan member's record, to the extent possible the plan member shall be given access to the remainder of the record after redacting/excluding the PHI the plan member was denied access to. The plan member shall be afforded the same appeal rights as outlined in section iv of this procedure.

iii) Approval of Request for Record Copy:

(1) The Port shall arrange for a mutually convenient time and place for the individual to inspect the PHI or obtain a copy or record summary consistent with the procedure below.

(2) The Port may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information if:

(a) The individual agrees in advance to such a summary or explanation; and

(b) The individual agrees in advance to the fees imposed, if any, by the Port.

(3) If an individual's request for access directs the Port to transmit the protected health information directly to another person designated by the individual, the Port must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identifies the designated person and where to send the copy of protected health information.

(4) If all or part of the record set is stored electronically and the plan member requests an electronic copy of his or her record, the Port shall provide the individual with access to the protected health information in the form and format requested by the individual, if the requested form and format can be readily produced.

(5) If the requested form and format cannot be readily produced, the Port shall provide the individual with access to the protected health information in a readable electronic form and format as agreed to by the Port and the individual.

(6) If part of the record is not stored electronically, a copy of this part of the record shall be made and provided in accordance with this procedure.

(7) The Port may charge a reasonable, cost-based fee for the copy of protected health information that includes only the following costs:

(a) Labor for copying, the protected health information requested by the individual, whether in paper or electronic form;

(b) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
(i) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
(ii) Preparing an explanation or summary of the protected health information, if agreed to by the individual.

iv) Denial of Request:
(1) The Port may deny or partially deny the plan member or personal representative access to the record if the Port determines, based on an assessment of the particular circumstances and based on current professional medical standards in the exercise of professional judgment that:
(a) The access requested is reasonably likely to endanger the life or physical safety of the plan member, or another person.
(b) The information requested refers to someone other than the plan member (unless the other person is a health care practitioner) and the access requested is reasonably likely to cause serious harm to that other person.
(c) Access to information requested by a personal representative of the plan member is reasonably likely to cause substantial harm to the plan member who is the subject of the information or to another person.

(2) Access may not be denied on the basis of the sensitivity of the health information.

(3) If the Port denies or partially denies the plan member access to the record for the reasons listed above, the plan member must be informed he or she has the right to have the denial reviewed by a designated licensed health care professional.

(4) If the Port denies or partially denies plan member access to certain PHI included in the plan member record, the Port shall give the plan member access to any other protected health information requested after excluding the protected health information as to which the Port has a ground to deny or withhold from access.

(5) If the Port denies or partially denies plan member access to certain PHI included in the plan member record, the plan member must be notified in writing. The notification must be retained for no less than six years.

(6) If the Port denies or partially denies access, the plan member must be provided with a written explanation of:
(a) The basis for the denial

(b) Instructions or procedures for lodging a complaint
(c) The plan member's right to appeal the denial or partial denial and how he or she may exercise this right
(d) Where to direct the request for access if the Port does not maintain the requested information and the Port knows where the requested information is maintained.

(7) Written notice regarding denial or partial denials of access must be provided to the plan member within 30 days of receipt of the plan member request.

(8) The denial or partial denial shall be documented in the record by placing a copy of the denial letter in the record.

(9) If the individual appeals a denial or partial denial, the appeal review request will be forwarded to the designated licensed health care professional acting as the reviewing official. The reviewing official must not have been directly involved in the original decision to deny access. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested. Upon completion of the review, The Port shall promptly provide the individual with written notice of the reviewing official's decision and otherwise carry out the decision in accordance with the requirements of the policy.

(10) The decision shall be documented by placing a copy of the denial or partial denial letter in the plan member's record.

c) Accounting for Disclosures. The HIPAA Privacy Rule requires all covered entities to account for any disclosures made on or after August 14, 2003 and retain the record of those disclosures for a period of six years. Plan members have a right to receive an accounting of disclosures made by the Port for purposes other than payment, and health care operations. Accounting includes any disclosure for purposes other than payment, health care operations, when specifically authorized by the plan member or the plan member's personal representative and limited exceptions (such as releases made during a criminal investigation). If a privacy or security breach occurs and plan member information is inappropriately or inadvertently released, this needs to be included in any accounting of disclosure. Disclosure accountings will not include disclosures:

- To the plan member who is the subject of the disclosure;
- Incidental to, or as part of, a permitted or required use or disclosure;
- Pursuant to a valid authorization;
- For certain, limited national security or intelligence purposes;
- To correctional institutions or law enforcement officials under certain circumstances;

- As part of a limited data set; or
- That occurred prior to August 14, 2003.

An accounting of disclosures will be maintained for six years from the date of the disclosure.

i) When an initial disclosure that needs to be accounted for is made (this includes inadvertent disclosures to an unauthorized third party), the Port will account for the disclosure in the plan member record

ii) When a trackable disclosure is made, the Port will include a brief statement of the purpose of the disclosure so that the plan member will be reasonably informed.

iii) If the Port receives a request for an accounting of disclosure, the Port will provide a copy of the Disclosure Log from the plan member record no later than 60 days after receipt of the request.

iv) If the Port is unable to meet the 60-day deadline, the Port may extend the deadline by no more than 30 days by informing the individual in writing, within the standard 60-day deadline, of the reason for the delay and the date by which the Port will provide the request. The Port may only extend the deadline one time per request for accounting.

v) If a health oversight agency or law enforcement request in writing that the Port suspend disclosure to the plan member that PHI has been disclosed to the law enforcement or health oversight agency, The Port shall agree to the suspension.
   (1) The agency or official must provide The Port with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities; and
   (2) The written statement must specify the time for which such a suspension is required.

v) The Port will track each accounting provided to a plan member in the plan member record by indicating in the record the date of the accounting and the purpose of the disclosure.

vi) The Port will provide one free accounting per 12-month period. For each additional request by a plan member within that period, the Port may charge a fee.

vii) If the Port elects to charge a fee, the Port will inform the plan member of the fee in advance and give them an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

d) Confidential Communications. Plan members have the right to request confidential or alternate means of communications. If a plan member requests that all communication be sent to an alternate address or location, the Port will comply with any reasonable request.

i) Review the request for confidential or alternate means of communication and determine if the request is administratively feasible.

ii) If it is not administratively feasible, contact the plan member and attempt to work with the plan member to establish a means of communication that is administratively feasible.

e) Request to Amend Record. Plan members have the right to request an amendment to their record. The Port is not required to honor amendment requests but needs to make amendments where appropriate. If the Port denies or partially denies the plan member's request to amend his or her record, the Port must allow the plan member the opportunity to rebut the denial.

i) The Port will request that plan members make requests for amendment in writing

ii) The Port will evaluate the request to determine if an error exists in the record and to determine if the Port created the initial record.

iii) If the Port created the record, the organization will decide to grant the amendment request, deny the request or partially deny the request.

iv) The Port may base a denial of the amendment request on the determination that the PHI that is the subject of the request for amendment:
(1) Was not created by the Port
(2) Is not part of a record or file that the Port maintains to make decisions about the plan member or would not otherwise be available for inspection by the Port
(3) Is accurate and complete

v) A written response will be sent to the plan member.
(1) The basis of denial will be included the written response to the plan member.

vi) Any written response regarding the denial or partial denial of an amendment shall include the plan member's rights to submit a rebuttal.

vii) Any written response regarding denial or partial denial of an amendment will also include a statement that, if the plan member does not submit a rebuttal, the plan member may request that the Port provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment.

viii) If the plan member submits a written statement disagreeing with the denial, the Port may reasonably limit the length of the statement of disagreement and, if appropriate, prepare a written rebuttal to the individual's statement. If the Port prepare a rebuttal, a copy will be provided to the plan member.

ix) If the amendment is denied and the plan member submits a written statement of disagreement, the statement, the Port's rebuttal, and denial or partial denial letter, or an accurate summary of these items, must be included with any subsequent disclosure of the PHI to which the disagreement relates.

x) If the request for amendment is accepted, the Port will make the appropriate amendment, identify the records that are affected by the amendment, and append or otherwise provide a link to the location of the amendment in the affected records.

xi) The Port will inform the plan member the amendment request has been accepted and will notify all other parties the amended portion of the record has been shared with of the amendment to the record.

xii) A copy of the plan member's initial amendment request and the Port's response shall be made a part of the member record.

xiii) The Port will include the following as part of the record:
(1) The plan member request for amendment
(2) The Port's denial or partial denial of the request
(3) The plan member statement of disagreement (if any)
(4) The Port's rebuttal (if any)

6) Organizational Requirements

a) Privacy Training.

i) Port employees who are considered part of the Port's plan sponsor "workforce" shall be trained to understand and implement the Port's privacy policies and procedures and the HIPAA Privacy Rule. Training shall occur:
(1) Within a reasonable time after employees become a member of the "plan sponsor" under the HIPAA Privacy Rule (*i.e.,* within 30 days of employment or transfer to a job with plan sponsor responsibilities).
(2) Within a reasonable time after material changes to the Port's privacy policies and procedures.
(3) Whenever, in the determination of the Port's Privacy Officer, additional training is necessary to ensure compliance with the Port's privacy policies and procedures or the HIPAA Privacy Rule.

ii) The Privacy Officer is responsible for the following:
(1) Identifying those employees who are subject to training, under the HIPAA Privacy Rule.
(2) Identifying the appropriate scope of such training.
(3) Conducting internal training for identified employees.

iii) Plan sponsor employees will be trained in the following areas:
(1) On the Port's HIPAA Privacy Rule policies and procedures, to the extent appropriate, for each employee in light of his or her job responsibilities;
(2) Permissible uses and disclosures of Protected Health Information;
(3) Relevant provisions of the HIPAA Privacy Rule; and
(4) The requirement that all employees report any use or disclosure of Protected Health Information that could be a violation of the Port's HIPAA Privacy Rule policies and procedures or the HIPAA Privacy Rule, whether such violation is caused by a workforce member or a service provider, to the Privacy Officer.

iv) The Privacy Officer or his/her designee will maintain records indicating who has been trained, what training occurred, and the date of training, for six years following the date of the training. These documents will be maintained in the Human Resources Department and will be retained in accordance with the Port's document retention policy.

b) Privacy Complaints
i) The Port's Privacy Officer will receive and respond to all complaints from health plan participants regarding the Port's compliance with the HIPAA Privacy Rule, unless a complaint relates to the Privacy Officer's conduct with

regard to compliance with HIPAA, in which case the Port's Legal Department shall receive and review such complaint.

ii) Upon receiving a complaint that there has been a violation of the Port's privacy policies or the HIPAA Privacy Rule, the Privacy Officer will investigate and take the following steps:
   (1) If the Privacy Officer concludes that the Port has not violated the Port's HIPAA policies and procedures or the HIPAA Privacy Rule, then the Privacy Officer will send a response form to the individual who submitted the complaint.
   (2) If the Privacy Officer determines that there has been a violation of the HIPAA Privacy Rule and/or the Port's HIPAA policy, either by the Port or a Port of Seattle employee, the Privacy Officer, shall:
      (a) Send a letter explaining what steps will be taken to correct any future improper uses or disclosures;
      (b) Determine whether there is any harm that should be mitigated, if practicable;
      (c) If the use or disclosure was by a Port plan sponsor workforce member, consider what sanctions should be imposed under Port's sanctions policy;
      (d) If the use or disclosure was by a service provider, determine whether further investigation or actions are necessary to ensure future violations do not occur;
      (e) Consider, in light of the nature of the improper use or disclosure of Protected Health Information, if additional training should occur for one or more employees; and
      (f) Consider, in light of the nature of the improper use or disclosure of Protected Health Information, whether any of the Port's policies or procedures need to be amended to ensure future violations do not occur.

iii) Documentation. All complaints and their disposition (*i.e.*, response letters) must be documented and retained for 6 years. These documents will be maintained by the Human Resources Department pursuant to the Port's document retention policy.

c) Privacy Violations
   i) If the Privacy Officer discovers that there has been an unauthorized or improper acquisition of Protected Health Information, in violation of the HIPAA Privacy Rule or the Port's policies and procedures regarding the same, the Privacy Officer shall take the following steps:

      (1) Determine whether such acquisition, access or use must be reported in order to comply with 45 CFR §164.400 et seq. A breach that must be reported is referred to as a "Reportable Breach."

(a) Except as described in subparagraphs (ii) or (iii), the Privacy Officer shall presume that any acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under 45 CFR Parts 160 and 164, Subpart E, is a Reportable Breach.

(b) The notice requirements of Section ii below do not apply to a breach that meets one of the following exceptions to a Reportable Breach:
1. An unintentional acquisition, access, or use of Protected Health Information by a Port workforce member or an individual acting under the authority of a business associate;
2. Inadvertent disclosure of Protected Health Information from one member of the Port workforce to another member of the Port workforce or from one person authorized to access Protected Health Information at a business associate to another person authorized to access Protected Health Information at the same business associate; or
3. Unauthorized disclosure in which an unauthorized person to whom Protected Health Information is disclosed would not reasonably have been able to retain the information.

(c) The notice requirements of Section ii below do not apply to a breach if the Privacy Officer determines that there is a low probability that the privacy or security of the Protected Health Information has been or will be compromised based on a risk assessment of at least the following factors:
1. The nature and extent of the Protected Health Information involved, including types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the Protected Health Information or to whom the disclosure was made;
3. Whether the Protected Health Information was actually acquired or viewed; and
4. The extent to which the risk to the Protected Health Information has been mitigated.

ii) The Privacy Officer will review his or her determination with the Legal Department. After receiving confirmation from the Legal Department that the unauthorized or improper acquisition, access, or use of Protected Health Information constitutes a Reportable Breach, the Privacy Officer shall provide the following notices as required by HIPAA and the regulations:

(1) A notice shall be provided to each individual whose Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the Reportable Breach without unreasonable delay and in no case later than 60 days after the date of

discovery of the Reportable Breach. Such notice shall include all of the following information:

(a) A description of the Reportable Breach, including the date of the breach and the date on which the breach was discovered;
(b) A description of the types of Protected Health Information that were involved in the Reportable Breach;
(c) Any steps the affected individuals should take to protect themselves from potential harm resulting from the Reportable Breach;
(d) A brief description of what the Plan is doing to investigate the Reportable Breach, mitigate harm to individuals and protect against any further breaches; and
(e) Contact procedures for individuals to ask questions or learn additional information (including a toll-free telephone number, an e-mail address, Web site, or postal address).

(2) For a Reportable Breach involving more than 500 residents of any one state or jurisdiction, notice shall be given to prominent media outlets serving the affected state or jurisdiction without unreasonable delay and in no case later than 60 days after the date of discovery of the Reportable Breach. The content of such notice shall be the same as in the notice to individuals described in Section (ii)(1).

iii) For a Reportable Breach involving more than 500 individuals, notice shall be given to the Department of Health and Human Services without unreasonable delay and in no case later than 60 days after the date of discovery of the Reportable Breach. The content of such notice shall be the same as in the notice to individuals described in Section (ii)(1).

iv) The Privacy Officer will maintain a log or other documentation of any Reportable Breaches involving fewer than 500 affected individuals and provide such documentation to the Department of Health and Human Services not later than 60 days after the end of the year in which such breaches occurred.

d) Sanctions for Violating the HIPAA Privacy Rule

i) If the Privacy Officer determines that as a result of the actions of a Port of Seattle employee there has been a violation of the HIPAA Privacy Rule or the Port's policies and procedures regarding the same, the Privacy Officer shall:

(1) Determine if the improper use or disclosure was intentional or unintentional;
(2) Determine if the improper use or disclosure was a one-time incident or a pattern or practice; and

(3) Determine if there are any mitigating factors (such as self-reporting or lack of proper training or supervision).

ii) The Port, at the written recommendation of the Privacy Officer outlining the factors above, will sanction any employee that uses or discloses a participant's or beneficiary's Protected Health Information in violation of the Port's privacy policies and procedures or in violation of the HIPAA Privacy Rule, in accordance with the Port's policy for employee discipline.

iii) Documentation. The Privacy Officer or his/her designee will maintain records showing the sanctions imposed under this policy for six years following the date the sanctions are imposed. These documents will be maintained by the Human Resources Department and will be retained in accordance with the Port's document retention policy.

e) No Retaliation or Intimidation

The Port will not retaliate against any participant or beneficiary who chooses to exercise his or her individual privacy rights, including the right to access Protected Health Information, the right to request amendment of Protected Health Information, the right to an accounting of disclosures, and the right to request certain privacy restrictions. The Port also will not intimidate any participant or beneficiary who seeks to exercise those rights. Further, the Port will not retaliate against or intimidate any person or organization that files a complaint regarding the Port's privacy practices with HHS, that participates in any investigation of the Port's privacy practices, or that opposes any act of the Port that allegedly violates the HIPAA Privacy Rule.

f) Mitigation of Harm Due to Improper Uses or Disclosures

i) The Port will mitigate, to the extent practicable, any harm caused by a use or disclosure of a participant's or beneficiary's Protected Health Information that is in violation of the Port's privacy policies and procedures or in violation of the HIPAA Privacy Rule.

ii) Upon learning of an improper use or disclosure by a plan sponsor workforce member or service provider, the Privacy Officer will take the following steps:
(1) Determine whether a participant or beneficiary could be or has been harmed by the improper use or disclosure;
(2) Determine whether there are any practicable steps that might have a mitigating effect with regard to the potential harm identified; and
(3) If so, implement the mitigating steps.

g) Business Associate Contracts

The Port has entered into business associate contract relationships with business associates as required by the HIPAA Privacy and Security Rules. Business associate contracts require that business associates maintain the privacy and security of the PHI stored, used or disclosed on behalf of the organization. Business associate contracts also require that business associates only use and disclose PHI for the purpose for which it was provided or as required by law.

All business associate contracts are periodically reviewed to reasonably ensure that business associates and their third-party vendors remain in compliance with state and federal law and to appropriately address legal risk to the Port. Contracts will be updated as necessary when business and regulatory requirements change.

i) All business associate contracts shall include the following requirements:
   (1) Not to use or further disclose PHI and other confidential information other than as permitted or required by the contract or as required by law.
   (2) Use appropriate safeguards to prevent use or disclosure of PHI and other confidential information other than as provided for by the contract.
   (3) Comply with all requirements of the HIPAA security rule, the use and disclosure provisions of the HIPAA privacy rule, and the breach notification rule.
   (4) Ensure that any subcontractors that create, receive, maintain, or transmit the organization's electronic protected health information on behalf of the business associate comply with all requirements of the HIPAA Security Rule.
   (5) Report inappropriate use or disclosure of PHI.
   (6) Report security incidents.
   (7) Report any breaches of PHI no later than 60 calendar days from the date the breach was discovered. Breach notification must include:
      (A) Individual's name and contact information
      (B) Nature/cause of breach
      (C) Date breach occurred and date breach was discovered
      (D) Information that was breached (e.g., social security number, name, address, medical condition, etc.)
      (E) Mitigating activity undertaken to limit damages
      (F) Security controls that will be implemented to reasonably ensure a similar breach does not occur in the future
   (8) Report any breaches of unsecured personal information other than PHI no later than 60 calendar days from the date the breach was discovered. Breach notification must include:
      (A) Individual names
      (B) A description of the incident in general terms
      (C) The approximate date of the breach of security
      (D) The type of unsecured personal information breached

(E) Brief description of what the business associate is doing to investigate the incident, mitigate damages and protect against like breached in the future

(9) Make its internal practices, books, and records relating to the use and disclosure of PHI received from; or received, created, used or disclosed on behalf of the Organization available to the Port and/or the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for purposes of determining the business associate's compliance with the HIPAA administrative simplification provisions statute and rules.

(10) Make every effort to mutually indemnify the other party. If one party is responsible for a breach or significant security or privacy incident, that party shall make every effort to hold the other party harmless for any inappropriate actions taken or inappropriate releases of information.

(11) At termination of the agreement, if feasible, business associate will return or destroy all PHI used or disclosed by business associate on behalf of the Port that business associate maintains in any form and will retain no copies of such information.

(12) If return or destruction is not feasible, business associate shall extend the contract privacy and security protections to PHI and limit further uses and disclosures to those purposes that make the return or destruction of PHI infeasible.

(13) Authorize the Port to terminate the agreement if the Port determines that business associate has or is violating any provision of the business associate contract, or alternatively, authorize an opportunity to cure said alleged material breach to the satisfaction of the Port within ten (10) days.