VENDOR / CONTRACTOR

# Privacy Basics

PREMERA | BLUE CROSS

# Introduction

Premera's mission is to provide our customers with peace of mind about their healthcare. This requires that everyone who works with or for Premera (the "Company") safeguard the protected personal information ("PPI") that our members entrust to us. This document provides you, as a Contractor, with a basic understanding of our privacy principles, terms and your responsibilities for conducting your work for the Company.

Protected Personal Information (PPI) means any and all information created or received by the Company that identifies or can readily be associated with the identity of an individual, whether oral or recorded in any form or medium, that relates to:

1. The past, present or future physical, mental or behavioral health or condition of an individual;
2. The past, present or future genetic information of an individual or their dependent, or relative of either;
3. The past, present or future payment for the provision of healthcare to an individual;
4. The provision of healthcare to an individual; or
5. The past, present or future finances of an individual, including, without limitation, an individual's name, address, telephone number, Social Security number, subscriber number or wage information.

All Contractors who provide goods or perform services for the Company must sign an agreement prior to doing business with the Company. As a new Contractor, you must know if your company is or is not a Business Associate (BA) of the Company, and whether you are entitled to have access to PPI. If you are unsure, ask your company. If your company is a BA, you must become familiar with and adhere to the terms of the Business Associate Agreement (BAA) with us. If your company is not a BA, but has a master services agreement with the Company, you must become familiar with and adhere to the privacy and security provisions of that document.

Our policies and procedures require compliance with federal and state privacy laws, including HIPAA privacy and security regulations. Contractors, too, must follow our policies and procedures and comply with all laws and regulations to which the Company is subject.

This document is organized based on whether you have access to PPI or not. If so, your Use and/or Disclose of PPI must be done carefully and in full compliance with our policies and procedures. Please refer to the Definitions section for any capitalized term in this document.

## Contractor with no approved access to PPI

### Breach Disclosure

You are responsible for ensuring that you do not Use or Disclose PPI in an unauthorized manner. If you accidentally do so, you must immediately report it to the Privacy Program. Reports must be sent via the Breach Reporting System (BRS) per the Confidentiality of Protected Personal Information procedure for the departmental in which you work. A link to the BRS can be found on **iHub**, by clicking "Company" and then selecting "Privacy".

## Contractors only using PPI within the Company and not disclosing PPI externally

### Need to know standard

PPI may be accessed, viewed, collected, or Used only to the extent necessary to perform your authorized job responsibilities and duties, as stipulated in the contract or BA with the Company.

### De-Identification of PPI

When your assigned job duties require that you handle PPI, you must evaluate whether or not the task can be accomplished using De-identified data or a Limited Data Set. If not, it is permissible for you to collect, Use or Disclose PPI.

### Use of PPI

It is vital for you to understand what "Use" of PPI are and what they mean to you while here at Premera. PPI may be collected or Used for routine business functions, applying the need to know standard. You are responsible for ensuring that you do not Use PPI in an unauthorized manner. However, in the event you accidentally do so, you must immediately report it to the Privacy Program. Reports must be submitted via the Breach Reporting System (BRS) pursuant to the Confidentiality of Protected Personal Information procedure for the departmental in which you work. A link to the BRS can be found on **iHub**, by clicking "Company" and then selecting "Privacy".

For those with no system access, please email the **privacyprogram@premera.com** or call **425-918-5531** or **425-918-5511.**

# Key privacy concepts for Contractors Using PPI and interacting with members, producers, groups or other entities external to the Company

## Need to know standard

PPI may be accessed, viewed, collected, or Used only to the extent necessary to perform your authorized job responsibilities and duties, as stipulated in the contract or BA with the Company.

## Minimum necessary standard

You may only Disclose or request a Limited Data Set or, if not practicable, the otherwise minimum amount of PPI necessary to perform your assigned job functions.

## Authentication and verification

When presented with a request for PPI, the first step you must take, prior to processing the request, is to authenticate the identity of the requestor and verify that they have authority to receive the PPI. You are required to follow the instructions for proper authentication, as specified in your area's departmental Confidentiality of PPI procedure.

It is important for those with external contact to remember that acknowledgement to the caller of the member relationship to the Company, prior to proper authentication, as well as failure to verify the caller's right to the PPI, are unauthorized Disclosures, in and of themselves.

When the law or the Company's Protected Personal Information Disclosure Tool does not allow a Use or Disclosure, the Company needs to receive, prior to the Use or Disclosure, a written specific authorization form signed by the individual or the individual's legal representative, if the individual cannot consent to the service under the law. In addition, if a written authorization is not on our corporate form, the Company's Complaints and Appeals Department must verify that it is valid, before information may be Used or Disclosed.

The Company may not Use, Disclose, or sell PPI for marketing purposes, unless a marketing authorization, signed by the individual or the individual's legal representative, is first obtained. Therefore, you cannot do so either.

## De-Identification of PPI

When your assigned job duties require that you handle PPI, you must evaluate whether or not the task can be accomplished using De-identified data or a Limited Data Set. If not, it is permissible for you to collect, Use or Disclose PPI.

## Use and Disclosure of PPI

It is vital for you to understand what "Use" and "Disclosure" of PPI are and what they mean to you while here are Premera. PPI may be collected, Used or Disclosed for routine business functions, applying the need to know and minimum necessary standards, unless an NDR is on file with the Company, in which case the terms of the NDR prevail. As NDRs apply only to family members and former providers, you must check for the existence of an NDR prior to Disclosure to such parties.

You are responsible for ensuring that you do not Use or Disclose PPI in an unauthorized manner. However, in the event you accidentally do so, you must immediately report it to the Privacy Program. Reports must be submitted via the Breach Reporting System (BRS) pursuant to the Confidentiality of Protected Personal Information procedure for the departmental in which you work. A link to the BRS can be found on **iHub**, by clicking "Company" and then selecting "Privacy".

# Who may receive PPI

PPI may be Disclosed to authorized representatives of a self-funded group who are specifically identified in the BAA with the Company. The EGRP or Employer Group Reporting Database provides the current authorized representatives for self-funded groups. However, unless De-identified or in response to either a Claims Status Inquiry or a specific authorization signed by the individual or the individual's legal representative, you may not Disclose PPI to insured groups, their producers or other designated representatives of the group.

No PPI may be shared with the plan sponsor of a self-funded or insured group health plan, except for:

1. Plan administrative purposes: Summary Health Information may be shared for purposes of the plan's obtaining bids from health plans for purposes of providing health insurance coverage under the group health plan; or modifying, amending, or terminating the group health plan; and
2. Enrollment and disenrollment of members onto or from the group health plan.

State and federal laws create special categories of third parties to whom, under certain circumstances, the Company may Disclose PPI. Contact your supervisor for guidance should you receive a request for PPI in this category.

# How PPI may be Used and Disclosed

You are responsible for ensuring that PPI within your control is handled in a confidential manner at all times, to prevent unauthorized Use and Disclosure, by following appropriate Company procedures.

## Use of removable computer media

You may not save data containing PPI to removable computer media. If PPI must be saved to media to support a business need, the IT Service Desk should be contacted for assistance at **84100.**

You are also responsible for following the Company's Records & Information Management Policy to ensure appropriate storage and disposal of PPI. PPI should not be stored on the Shared Common drive. Records containing PPI are to be stored in secure folders with access limited to those having a business need to know. You are responsible for verifying with Information Security Administration that your shared drive folders are secure, prior to saving PPI in them.

## Transmission of PPI

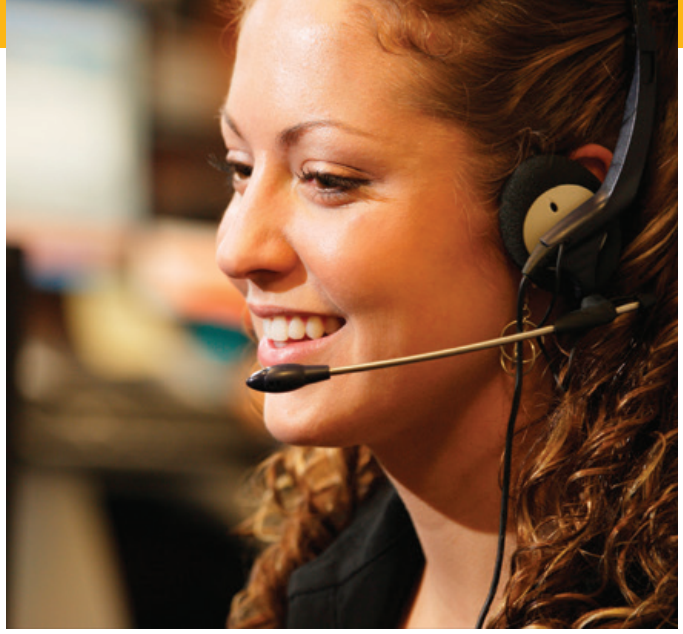
Any electronic transmission of PPI must be done with extreme caution. Messages should include only the minimum necessary information for the intended purpose and be addressed or forwarded only to those individuals to whom our policies and the law allow Disclosure, and who have a need to receive the confidential information.

PPI may be transmitted safely within the PREMERA family of companies. This includes communications to and from users who are traveling or telecommuting, as long as the communication is via their PREMERA email address (i.e., premera.com, lifewise.com, etc.), PREMERA's instant-messaging system, or another form of electronic communication that is controlled by the Company.

Because Internet connections outside of the Company are not secure and are susceptible to tampering, additional restrictions apply to the transmission of PPI outside of the Company. Emails containing PPI may be sent to non-Company email addresses only via secured mechanisms that have been formally approved by Information Security. PPI may never be sent to either an internal or external recipient via an Internet file-transfer ("cloud") service Web site. Uses or disclosures of PPI data that are allowed by our corporate policy, but that are too large to be transferred by confidential email, should be done through the Electronic Transmission Center. Contact the ETC mailbox. Documents containing PPI may be faxed to authorized recipients as long as senders follow their department's Confidentiality of PPI procedure. SMS text messaging, non-Company instant-messaging applications, social media and microblogging services, and other electronic communication mechanisms that are not controlled by the Company may not be employed for the transmission of PPI.

# Definitions

Important note: The following terms have specific meaning and are capitalized when used in this document. You must understand the meaning of each term as you read this document so as to fully understand its provisions.



**Breach** means an unauthorized acquisition, access, Use or Disclosure of unencrypted/unsecured PPI that poses more than a low probability of compromise to the PPI, as determined by the Company.

**Business Associate** means a person or entity that creates, receives, maintains, or transmits PPI in the performance of a function or activity for the Company: e.g., pharmacy benefit manager, disease management Vendor, consultants, Contractors, third-party administrators, auditors, lawyers, etc. It does not include all Contractors providing services to Premera.

**Business Associate Agreement** is an addendum to the master services agreement that binds the Business Associate to specific privacy and security obligations.

**Claims Status Inquiry (CSI):** An inquiry to determine the status (e.g., received, in-process, fully adjudicated or under appeal) of a health care claim, for which the Company must receive, from the requestor, prior to any acknowledgement of the person as a Premera member or the existence of a claim: (1) the date of service (month and year), (2) the type of procedure the member had done, and (3) the name of the provider of service.

**Company** means the PREMERA entity in possession of the PPI, including Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, LifeWise Health Plan of Washington, LifeWise Health Plan of Oregon, or LifeWise Assurance Company in regard to Student Insurance, or any of PREMERA's subsidiaries or affiliates.

**Contractor or Vendor:** A third party that performs services for the Company, including Business Associates, and that may have a written contract with the Company that includes confidentiality provisions that safeguard PPI. All employees of these third parties that have access to The Company's PPI are required to sign an attestation that they have read, understand and agree to comply with the Company's policies.

**De-Identification of PPI** means the removal or other form of elimination or concealment of types of information, as outlined below, that could enable the identification of PPI to a particular Individual. The types of information that must be de-identified include name, address, zip code, names of relatives, names of employers, birth date, telephone number, fax number, electronic mail address, Social Security number, medical record number, health plan member number, account number, certificate/license number, any vehicle or other device serial number, Web universal resource locator (URL), Internet protocol (IP) address number, finger or voice prints, photographic images, and any other identifying number, characteristic or code.

**Disclose / Disclosure** means to release, transfer, provide access to, or divulge in any other manner PPI outside the Company.

**Limited Data Set** is PPI from which the following direct identifiers have been removed: names (including the individual's name and names of relatives, employers and household members; addresses; telephone numbers; fax numbers; email addresses; medical record numbers; health plan numbers; Social Security numbers; account numbers; certificate/ license numbers; vehicle identifiers such as serial and license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) addresses; biometric identifiers including finger and voice prints; and photographs. Elements of dates, such as birth dates and zip codes, are allowed to remain.

**Non-Disclosure Request (NDR)** is a PREMERA member's request to prohibit the Disclosure of PPI to a specific person who would normally have access to such PPI. A Non-Disclosure Request:

1. Specifies the person to whom PPI should not be Disclosed; and
2. Specifies the address to which any correspondence for the member containing PPI should be sent.

NDR Requests will only be accepted for personal safety reasons in which the member has certified that the Disclosure of all or part of the PPI would endanger them or their minor children (as applicable). NDR request forms are not for requesting a change of address or alternate address for reasons that do not involve personal safety.

**Summary health information** means information, that may be individually identifiable health information, and: (1) that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and (2) from which the following elements have been removed: names (including the individual's name and names of relatives, employers and household members; addresses (except five-digit zip code); dates (except year); telephone numbers; fax numbers; email addresses; medical record numbers; health plan numbers; Social Security numbers; account numbers; certificate/license numbers; vehicle identifiers such as serial and license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) addresses; biometric identifiers including finger and voice prints; and photographs.

**Use** means to employ, apply, utilize, examine, or analyze PPI within the Company.

## Violations of Company privacy or security policy

Violations by a Business Associate, Contractor or Vendor may be grounds for termination of the business relationship.

## Attestation of understanding

I have read and I understand Premera's Vendor/Contractor Privacy Basics, effective March 2014, and I agree to abide by its contents.

_____

Signature

_____

Printed Name

_____

Date

(Rev. March 2014)

PREMERA BLUE CROSS

An Independent Licensee of the Blue Cross Blue Shield Association