NOTICE OF PRIVACY PRACTICES & REQUIRED DISCLOSURES

(Effective Date: 09/12/2025)

THIS NOTICE DESCRIBES HOW PROTECTED INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION, ALONG WITH DISCLOSURES WE ARE REQUIRED TO PROVIDE. PLEASE REVIEW IT CAREFULLY.

PURPOSE OF THIS NOTICE

This Notice of Privacy Practices ("Notice") is intended to comply with the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA"). This Notice describes our privacy practices with regards to individually identifiable health information protected by HIPAA and non-public personal, financial and health information protected by GLBA ("Your Protected Information").

OUR PRIVACY OBLIGATIONS

We are required by federal and state law to protect the privacy of Your Protected Information and to provide you with this Notice of our legal duties and privacy practices. When we use or disclose Your Protected Information, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use of disclosure). We are also required to comply with applicable state privacy laws, including the Washington My Health My Data Act, which establishes specific rights for Washington residents regarding consumer health data.

HOW WE PROTECT YOUR PROTECTED INFORMATION

We treat Your Protected Information in a confidential manner. Our employees are trained and required to protect the confidentiality of Your Protected Information. Employees may access Your Protected Information only when there is an appropriate reason to do so, such as to administer or offer our products or services. We also maintain physical, electronic and procedural safeguards to protect Your Protected Information as required by applicable laws. In addition, we employ enhanced technical safeguards consistent with current federal guidance, including:

- Encryption of data at rest and in transit
- Multi-factor authentication for system access
- Regular risk assessments and penetration testing
- Workforce training on phishing and social engineering threats

HOW WE COLLECT YOUR PROTECTED INFORMATION AND THE TYPES OF YOUR PROTECTED INFORMATION WE COLLECT

The information that you give us when applying for our products or services generally provides all of Your Protected Information we will need. If we need to verify Your Protected Information or need additional information, we may obtain Your Protected Information from third parties such as Medicare, adult family members, employers, other insurers, consumer reporting agencies, physicians, hospitals, and other medical personnel. Your Protected Information collected may relate to your finances, employment, health, vocations or other personal characteristics as well as transactions with us or with others.

OUR USES AND DISCLOSURES OF YOUR PROTECTED INFORMATION

How We Use Your Protected Information: We collect and use Your Protected Information for business purposes with respect to our products, services and other business relationships involving you. We may disclose any of Your Protected Information, within acceptable regulatory limitations, when we believe it necessary for the conduct of our business, or where disclosure is required or permitted by law. For example, Your Protected GLBA Information may be disclosed to others, including to our service providers to help us process your applications or service your accounts. Our service providers may include Insurance Carriers, the Department of Health and Human Services, Medicare, the Federally Facilitated Health Insurance Marketplace, or any other agency involved in obtaining the insurance coverage you have chosen. Your Protected GLBA Information may be disclosed to others that are outside of our company, such as companies that provide technical, computer or marketing services for us. We may also provide your name and address to companies that perform marketing services on our behalf, limited to only that information which we deem appropriate for these service providers to carry out their functions. We do not provide Your Protected GLBA Information to any company whose products and services are being

marketed unless you authorize us to do so. These companies are not allowed to use this information for purposes beyond your specific authorization.

Uses and Disclosures of Your Protected Information for Payment and Healthcare Operations: We may use and disclose Your Protected Information to others as necessary to pay your healthcare provider(s) for health benefits covered by your plan or for other healthcare operations necessary to provide these health benefits to you, without your express, implied or specific consent or authorization. In addition, and without limitation, we may use and disclose Your Protected Information to others as follows:

1. Payment. We may use and disclose Your Protected Information to obtain payment of our commissions or other compensation and to determine and fulfill our responsibility to provide health benefits under your plan, for example, to assist in the administration of benefits or facilitate payment of claims.
2. Business Operations. We may use and disclose Your Protected Information for our business operations, for example, to do business planning, provide customer service and conduct quality assessment and improvement activities.

We are prohibited, by federal law, from using or disclosing genetic information for underwriting purposes in all circumstances.

Uses or Disclosures of Your Protected Information with Your Authorization: Outside of the requirements for payment, healthcare operations and treatment, most uses and disclosures of Your Protected Information will only be made if you give us your written authorization ("Your Authorization"). This includes most uses and disclosures of psychotherapy notes, uses and disclosures for marketing purposes (including subsidized treatment communications), disclosures that are considered a sale of Your Protected Information, and any other uses and disclosures not described below. You may revoke Your Authorization, except to the extent that we have acted in reliance on it, by delivering a written revocation statement to our Privacy Officer.

Uses and Disclosures of Your Protected Information Without Your Consent or Authorization:

- *As Required by Law.* We will use or disclose Your Protected Information when required to do so by federal, state or local law. Please note, we are required by law to keep copies of our records for a minimum of ten (10) years.
- *Business Associates.* We may disclose Your Protected Information to our Business Associates that perform functions on our behalf or provide us with such functions or services. For example, we may use another company to perform computer or technical services for us. All of our Business Associates are obligated by law and under contracts with us to protect the privacy of Your Protected Information and are not allowed to use or disclose any information other than as specified in our contract.
- *Marketing Communications.* We may use and disclose Your Protected Information for marketing communications made by us to you only as permitted by law.
- *Public Health Activities.* We may disclose Your Protected Information for the following public health activities and purposes: (1) to report health information to public health authorities for the purpose of preventing or controlling disease, injury or disability; (2) to report child abuse or neglect to the government authority authorized by law to receive such reports; and (3) to alert a person who may have been exposed to a communicable disease.
- *Victims of Abuse, Neglect or Domestic Violence.* We may disclose Your Protected Information if we reasonably believe you are a victim of abuse, neglect or domestic violence to the appropriate state agency as required or permitted by applicable state law.
- *Health Oversight Activities.* We may disclose Your Protected Information to a government agency that oversees the healthcare system or ensures compliance with the rules of government health programs such as Medicare or Medicaid.
- *Lawsuits and Disputes.* We may disclose Your Protected Information in the course of a judicial or administrative proceeding in response to a legal order or other lawful process.
- *Law Enforcement.* We may disclose Your Protected Information to a law enforcement official as required by law or in compliance with a court order or other lawful process.
- *Health or Safety.* We may disclose Your Protected Information to prevent or lessen a serious or imminent threat to a person's or the public's health or safety.
- *Specialized Government Functions.* We may disclose Your Protected Information to units of the government with special functions, such as any branch of the U.S. military or the U.S. Department of State.
- *Workers' Compensation.* We may release Your Protected Information for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.
- *Individuals Involved with Your Healthcare.* We may use or disclose Your Protected Information in order to tell someone responsible for your care about your location or condition. We may disclose Your Protected Information to your

relative, friend or other person you identify, if the information relates to that person's involvement with your healthcare or payment for it.

YOUR INDIVIDUAL RIGHTS

- *Right to Inspect and Copy.* You may request access to our records that contain Your Protected Information in order to inspect and request copies of the records. We will provide access to your information within 30 days of your request, unless permitted by law to extend by an additional 30 days, in which case you will be notified in writing. Under limited circumstances we may deny you access to a portion of our records of Your Protected Information. If you desire access to our records of Your Protected Information, please obtain a record request from our Privacy Officer and submit the completed form to the Privacy Officer. If you request copies, we may charge you copying and mailing costs. You have a right to receive a copy in electronic format, if so requested. Please see our Notice of Pricing for PHI Records on our website valleyinsurancepro.com.
- *Right to Amend*. You have the right to request that we amend Your Protected Information maintained in our enrollment, payment, claims adjudication and case or medical management records or other records used, in whole or in part, by or for us to make decisions about you. If you desire to amend these records, please obtain an amendment request form from our Privacy Officer. We will comply with your request unless special circumstances apply. If your physician or other healthcare provider created the information that you desire to amend, you should contact the provider to amend the information.
- *Right to an Accounting of Disclosures.* Upon request, you may obtain an accounting of certain disclosures of Your Protected Information made by us, excluding disclosures made earlier than six years before the date of your request. The first list you request within a 12-month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.
- *Right to Request Restrictions.* You may request restrictions on our use and disclosure of Your Protected Information for payment and healthcare operations in addition to those explained in this Notice. While we will consider all requests for such additional restrictions carefully, we are not required to agree to all requested restrictions but will comply with legally required restrictions. We also comply with federal rules that prohibit information blocking and support the timely, interoperable exchange of health information. If you wish to request additional restrictions concerning Your Protected Information, please obtain a request form from our Privacy Officer and submit the completed form to the Privacy Officer. We will send you a written response.
- *Right to Request Confidential Communications.* We accommodate any reasonable request for you to receive Your Protected Information by alternative means of communications or at alternative locations.
- *Right to Receive Paper Copy of this Notice.* Upon request, you may obtain a paper copy of this Notice.
- *Right to Receive Security Breach Notification.* We will inform you if there is a breach of security related to Your Protected Information.
- *Right Not to Provide Requested Information.* You may choose not to provide us with the requested information, however, your failure to provide such information may result in our inability to assist you.
- *Verification of Identity.* In keeping with our privacy standards, all requests to view, copy, amend, correct, substitute, or delete your Protected Information requires verification that the requesting individual or individual's legal authority has permission to access this information. The requester must submit through mail, via an electronic upload process, or in-person, a copy of one of the following government-issued identifications: a driver's license, school identification card, voter registration card, U.S. military card or draft record, identification card issued by the federal, state or local government, including a U.S. passport, military dependent's identification card, Native American tribal document, or U.S. Coast Guard Merchant Mariner card. If the requester cannot provide a copy of one of these documents, he or she can submit two of the following documents that corroborate one another: a birth certificate, Social Security card, marriage certificate, divorce decree, employer identification card, high school or college diploma, and/or property deed or title. If the request for information is from anyone other than you, a valid power of attorney will be required.
- *Washington Residents – Additional Rights.* If you are a resident of Washington, you have additional rights under the My Health My Data Act (MHMD):
    - Right to Know: You may request a list of the categories of consumer health data we collect, how it is used, and with whom it is shared.
    - Right to Deletion: You may request deletion of consumer health data that is not required for legal, contractual, or business purposes.
    - Right to Withdraw Consent: If you have previously provided consent for certain uses of consumer health data, you may withdraw it at any time.
    - Geofencing Protections: We do not use geofencing technology around healthcare facilities.

These rights apply to consumer health data that may not be covered under HIPAA but is protected under Washington law. To exercise these rights, please contact our Privacy Officer using the information provided in this Notice.

THIRD-PARTY TECHNOLOGY USE

We do not disclose Protected Health Information through online tracking technologies such as cookies, analytics tools, or pixels. If we use website or marketing tools, they are configured not to collect or share health-related information. Any third-party services we engage with are subject to privacy safeguards and, where applicable, business associate agreements.

CHANGES TO THIS NOTICE

We reserve the right to change this Notice and to make the revised or changed Notice effective for Your Protected Information we already have as well as any of Your Protected Information we receive in the future. We will post the current notice at our office location with its effective date on the first page. You are entitled to a copy of the Notice currently in effect. We will inform you of any significant changes to this Notice. This may be through our newsletter, a sign prominently posted at our location(s), a notice posted on our website or other means of communication.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with our office, or with the Secretary of the Department of Health and Human Services at:

Office for Civil Rights – Pacific Region
U.S. Department of Health and Human Services c/o Regional Manager
90 7th Street, Suite 4-100, San Francisco, CA 94103
Customer Response Center: (800) 368-1019 | Fax: (202) 619-3818 | TDD: (800) 537-7697 Email: ocrmail@hhs.gov |
Complaint Portal: https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

To file a complaint with us, contact our Privacy Officer as provided below. You will not be penalized for filing a complaint.

If you have any questions about this notice, please contact our Privacy Officer at: (503) 480-0499 or toll free at (855) 999-9847, or by mail at 437 Union St. NE, Salem, Oregon 97301.

OUR POLICY REGARDING DISPUTE RESOLUTION

Any controversy or claim arising out of or relating to our privacy policy, or the breach thereof, shall be settled by arbitration in accordance with the rules of the American Arbitration Association, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

OPT OUT

We do not sell or share your personal information with third parties for marketing or promotional purposes. Your information is only used to communicate with you about services provided by Valley Insurance Professionals. However, from time to time we may let you know about discounts, products and services that are available to you. If you would like us not to contact you, you may opt out by sending a signed and dated request to: Valley Insurance Professionals, Attn: Opt Out, 437 Union St. NE, Salem, Oregon 97301. You may also request a Privacy Policy Opt-Out form by calling (503) 480-0499 or toll free at (855) 999-9847.

DISCLOSURES

The Consolidated Appropriations Act of 2021 (CAA): The CAA was enacted on December 27, 2021. Title I (No Surprises Act) and Title II (Transparency) of Division BB of the CAA amended Title XXVII of the PHS Act by establishing new protections for consumers related to surprise billing and transparency in health care. The CAA contains new requirements for health insurance issuers in the individual and group markets, health care providers and facilities, and providers of air ambulance services. One benefit of the CAA is the No Surprises Act, which protects people covered under group and individual health plans from receiving surprise medical bills when they receive most emergency services and non-emergency services from out-of-network providers at in-network facilities, and services from out-of-network air ambulance service providers. In addition to other rules, the Transparency in Coverage Rule (TCR) requires that hospitals publish standard charges for the most common services, accessible in a consumer- friendly format, so consumers can research, compare, choose providers, and make health care decisions while knowing the cost of these services before receiving care. As part of the CAA, insurers, agents, brokers, and consultants who work in the health benefits field are required to disclose compensation, whether received directly or indirectly, for any payments that equal $1,000 or more, or non-cash compensation that equals $250 or more.

As agents and brokers, we at Valley Insurance Professionals, receive a commission from Insurance Carriers for the services we provide assisting consumers with understanding the insurance products available to them, education on specific plans to meet your needs, and enrollment into the plan(s) you have chosen. Our compensation never comes directly from consumers, and we are not only obligated but fiercely dedicated to providing objective assistance in a way that our clients have peace of mind and feel confident knowing they have found the right coverage at an affordable price and a trusted partner who will be there to answer all their questions. We believe you deserve to really understand your insurance options so you can feel confident that you are getting the right coverage without breaking your budget.

At Valley Insurance Professionals we offer a broad range of insurance products from multiple carriers. Each product and each carrier have their own commission schedule. The CAA requires that agents and brokers disclose the commission amounts for any plans that fall under the ERISA guidelines (these are typically group employer plans). We wanted to go a step further and disclose the range of commissions we may receive for some of our most common insurance types. For example, for a dental plan from one carrier, we may receive a commission of $2.00 per member per month (PMPM); another carrier offers $3.00 PMPM, while another pays $2.50. Individual and family health insurance plans through the Marketplace, or directly through a carrier, pay the same commission whether a consumer chooses a Bronze plan, Silver plan or Gold plan, but each carrier pays differently. For example, one may pay $16.00 PMPM, while another may pay $18.00. Some of our carriers have paid bonuses if we enroll a certain number of new people during open enrollment, while another carrier pays an extra $1.00 PMPM if the agent or broker goes through additional training and credentialling, to better understand their products.

There are too many products and scenarios to list in this disclosure, but if you are interested in what the commission may be for the products we assist you with, please do not hesitate to contact our office at (503) 480-0499. Please know, as a local independent insurance agency, we have access to numerous carriers which allows us to prioritize the right solution for your individualized needs. We take the time to do the shopping for you, looking at the total package so we can recommend the best option with the most savings, and we do this, always, with your best interest at heart, not the amount of the commission.

HIPAA Privacy Rule Update Effective June 25, 2024. The Department of Health and Human Services (HHS) issued a final rule to modify the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). HHS issued this final rule after careful consideration of all public comments received in response to the notice of proposed rulemaking for the HIPAA Privacy Rule to Support Reproductive Health Care Privacy (“2023 Privacy Rule NPRM”). This final rule (“2024 Privacy Rule”) amends provisions of the Privacy Rule to strengthen privacy protections for highly sensitive PHI about the reproductive health care of an individual, and directly advances the purposes of HIPAA by setting minimum protections for PHI and providing peace of mind that is essential to individuals' ability to obtain lawful reproductive health care. This final rule balances the interests of society in obtaining PHI for non-health care purposes with the interests of the individual, the federal government, and society in protecting individual privacy, thereby improving the effectiveness of the health care system by ensuring that persons are not deterred from seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which such health care is provided.

You may be asking, what does this mean to me? First, this update to the Privacy Rule will be handled differently by every entity that interacts with your private information. A doctor or clinic may have different requirements, based on the level of personal information they store about you. As your insurance agent, we may discuss the types of prescriptions you take, doctors you see, or hospitals/clinics you prefer. During these conversations, you may share sensitive information with us about your health or the health of a family member. The updated Privacy Rule states that we cannot share your sensitive information, specifically about your reproductive health care, to anyone who is trying to conduct or impose, a criminal, civil or administrative investigation, or liability, on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care. The update also states that before any information can be disclosed, you, as the consumer, would need to sign an attestation allowing this information to be released. If you want to learn more about the changes to the Privacy Rule, you can visit the National Archives Federal Register at federalregister.gov and search for HIPAA Privacy Rule To Support Reproductive Health Care Privacy. You will find the sections of the Rule that have been updated along with an Executive Summary and a synopsis of comments and responses.