PDS HEALTH CALIFORNIA EMPLOYEE AND APPLICANT PRIVACY NOTICE

Last Updated and Effective on June 24, 2025

PDS Health (the "Company," "we," or "us") has developed and implemented this privacy policy ("California Employee Privacy Notice") to demonstrate its commitment to privacy for California residents who are or are seeking to become a member of the Company's workforce. This California Employee Privacy Notice is designed to assist California workforce members and candidates ("you") in understanding how we collect, use, share, and safeguard personal information as part of your working relationship with us.

To Whom this Workforce Member Privacy Policy Applies

This California Employee Privacy Notice applies to individuals in connection with their status as a workforce member or candidate (collectively "workforce members"). Our privacy practices with respect to personal information collected in other contexts, including visiting any of the PDS Health websites, can be found in the privacy policy or notice posted on those websites. Please review those privacy policies to learn more about our privacy practices generally.

Except as may be specifically required by law, this Workforce Member Privacy Policy does not apply to information available from a public source (such as a telephone directory) or to aggregated or de-identified information we may collect about our workforce, nor to references to workforce members in company work product. This Workforce Member Privacy Notice is intended to comply with the California Consumer Privacy Act ("CCPA"), as updated by the California Privacy Rights Act ("CPRA").

1. Updates

This Notice will be updated from time-to-time to reflect changes in our business, legal or regulatory obligations, so please check this Notice periodically for changes by visiting http://www.pdshealth.com. We will not collect additional categories of your personal information or use your personal information already collected for additional purposes without providing you with a notice of our intent to do so. Any changes to this Notice will be effective on the date we post the updated Notice to our website.

2. Definitions:

"Workforce member" or "you" means an identified or identifiable natural person who is a California resident and who is acting as a PDS job applicant, employee, or contractor. In this context "job applicant" refers to any person who has submitted his or her candidacy with PDS; "employee" refers to any person who is or was previously employed at PDS as a full-or part-time employee, temporary worker, owner, director, or officer; and "contractor" means a natural person who provides any service to a business pursuant to a written contract.

"**Personal information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. Personal information does not include publicly available information or information that has been de-identified.

3. Notice at Collection

At or before the time of collection, you have a right to receive notice of our practices, including the categories of personal to be collected, the purposes for which such information is collected or used, whether such information is sold or shared and how long such information is retained. You can find those details below.

4. Categories of Personal Information We Collect About You

We may collect the following categories of personal information about you:

- **Identifiers:** This includes a real name; postal address; email address; phone number; emergency contact details; online account name and password; security question and answer; birth certificate; children's names; parents' names; mother's maiden name; marriage license; death certificate; passport number; national identification number; driver's license number; social security number; tax ID number; government identification card number; immigration/naturalization number; retirement account number; beneficiary number; and National Provider Identifier (NPI).

  ***Note*:** Some of these categories of personal information are also deemed Customer Records under California and so will be included in the chart below as such.

- **Protected Classifications:** This includes age; gender; birthplace; nationality; racial or ethnic origin; citizenship status; marital status; family information; pregnancy; disability status; criminal history; drug test results; tobacco use indicator; veteran status; health and medical information.
- **Commercial information:** This includes vehicle make and model; vehicle license plate number.
- **Biometric Information:** This refers to facial images/photographs; shirt size; height; and weight.
- **Internet/Network Activity**. This refers to your interactions with Internet-connected devices we control and use of our networks. This category includes the browsing and search history on Company-owned or controlled networks, software usage logs, and other information related to your use of Company-owned or controlled devices, networks, and software applications.
- **Geolocation Data:** This refers to general location information including that collected from mobile devices and vehicles.
- **Sensory Data:** This includes audio, electronic, or visual information; which may include video surveillance information; photographs; and other audio-visual information.
- **Professional or Employment-Related Information:** This includes professional or employment-related information, such as job title/role; employment identification number; company/entity; office location; business unit/division; line/reporting manager; employment status; start date; end date and reason for termination; exit interview; hours of work; record of absence/time tracking/annual leave; employment history; employment contract type; benefits and entitlements information; health and safety related information and reporting; performance rating; disciplinary action; grievances and complaints; salary/wage information; salary/wage expectation information; bonus payments; tax information; expense and reimbursement information; workers compensation claims; job application details; resume information; previous work history; and other employment information; professional memberships; professional licenses; qualifications/certifications; malpractice insurance information; DEA certificate and number; professional references; aptitude assessment results; LinkedIn profile information; and resume cover letter.
- **Education information**: This includes education history; educational degrees; academic transcripts/grades; training history; languages; and certifications/courses.
- **Inferences** drawn from other personal information that is used to make decisions about an individual. This includes information reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- **Sensitive Personal Information**. The CCPA defines various categories of personal information as "sensitive personal information," including government IDs; precise geolocation; payment card and bank account information, demographic information; email contents (when PDS is not the recipient); biometric information; and health information.

To clarify what categories of personal information we collect and the sources from which we collect them, as well as if we share or sale this personal information, we have provided the following chart. You can learn more about our specific practices by reading our more detailed disclosures below the chart.

Categories of Personal Information	Categories of Sources from which the Information was Collected	Categories of Third Parties to whom this type of Personal Information is Disclosed for a Business Purpose	Types of Third Parties with Whom this Category of Personal Information Is Shared/Sold
Identifiers	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	We do not sell or share
Customer Records (as defined in Cal. Civ. Code § 1798.80(e))	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	We do not sell or share
Protected Classifications	• Workforce Members • Candidate Recruiting Partners • Governmental Entities • Company Affiliates	• Workforce Members • Company Affiliates • Human Resources Service Providers • Business Operations Service Providers • Candidate Recruiting Partners • Governmental Entities	We do not sell or share
Commercial Information	We do not collect commercial information in the context of a workforce member relationship.		We do not sell or share
Biometric Information	• Workforce Members	• Workforce Members • Business Operations Service Providers	We do not sell or share

Internet/Network Activity	• Workforce Members • Business Services Providers	• Workforce Members • Business Services Providers • Company Affiliates • Human Resources Service Providers	We do not sell or share
Geolocation Data	We may gather your geolocation based on your address, IP address, or other data associated with a particular location. If you are using company-equipment that collects geolocation, we may associate that geolocation with you.	• Workforce Members • Business Services Providers • Company Affiliates • Human Resources Service Providers	We do not sell or share
Sensory Data	We may collect your image, voice, electronic activity, or other sensory data through recording devices such as a security camera or call recording device.	• Workforce Members • Business Services Providers • Company Affiliates • Human Resources Service Providers	We do not sell or share
Professional or employment-related information	• Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Governmental Entities	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	We do not sell or share
Education Information	• Workforce Members • Educational institutions • Candidate Recruiting Partners	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	We do not sell or share
Inferences drawn from other personal information	We do not collect inferences, but we may make inferences about workforce members based on the personal information we have	We do not disclose inferences we make outside of the company, but we may store inferred personal data with our Business	We do not sell or share

	collected. For example, we may make inferences regarding a workforce members' suitability for a particular position or task.	Service Providers (for example, our cloud storage providers).	
Sensitive Personal Information	• Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	• Workforce Members • Company Affiliates • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Governmental Entities	We do not sell or share

We collect personal information about our workforce members from a variety of sources, but primarily from the workforce members themselves. In addition, we gather personal information through workforce members' interaction with the Company's systems and personnel, and we receive personal information from third parties who provide it to us. The following is a list of the sources from which we may collect personal information.

- **Candidate Recruiting Partners**. These are the persons or entities who assist in facilitating recruitment and review of candidates to become workforce members. These entities include recruiting firms, job search services, social media companies (e.g., LinkedIn), and professional recruiting agents. We may also collect personal information from any other person or entity with whom you provide a reference, including past employers, personal references, former colleagues, and others.
- **Human Resources Service Providers**. These are the persons or entities who assist in providing human resources and workforce management services, including background check providers, human resources software services providers, insurance providers, employee payment and benefits providers, governmental entities, and similar entities.
- **Business Services Providers**. These are those persons or entities with whom we have a relationship to provide business operations services and support to the Company. These providers may include the following:
    - **IT Operations Providers**. These include cloud computing service providers, internet service providers, data backup and security providers, functionality and infrastructure providers, and similar service providers.
    - **Professional Service Providers**. These include lawyers, accountants, consultants, security professionals, and other similar parties when disclosure is reasonably necessary to comply with our legal and contractual obligations, prevent or respond to fraud or abuse, defend ourselves against attacks, or protect the rights, property, and safety of us, our customers, and the public.
    - **Operations Providers.** These include service provider with whom we partner to provide day-to-day business operations, including real estate advisors, event planners, food services providers, entertainment providers, payment processors, banks, facilities management providers.

- **Affiliates.** Our affiliates include our parent company, subsidiaries, joint venturers, or other companies that we control or that are under common control with us.
- **Governmental Entities**: These are governmental agencies that may provide information about workforce members.

We may also collect personal information from any other person or entity with whom you interact in the scope and course of a workforce members affiliation with the Company. For example, we may collect personal information about you from customers, business contacts, and the public.

5. The Purposes for Which Your Personal Information Is Collected or Used

We may collect or use personal information from you for the following business purposes:

PDS collects the personal information identified in Section 4 above for the reasons listed below.

- *To Process Employment Applications and Onboard New Hires*, including to conduct employment related background screening and checks; and recruiting.
- *To Credential Healthcare Practitioners,* which includes both employee practitioners and independent contractor practitioners for participation on insurance carrier and managed care plan provider panels, including any legally required reporting to, and queries of, national provider data banks.
- *To Administer Benefits*, such as medical, dental, vision, wellness, EAP, life, retirement benefits, and reimbursement and assistance programs, including recording and processing eligibility of dependents, absence and leave monitoring, insurance and accident management.
- *To Pay and Reimburse for Expenses*, including salary administration, payroll management, payment of expenses, to administer other compensation related payments, including assigning amounts of bonus payments to individuals.
- *To Conduct Performance-Related Reviews*, including performance appraisals, career planning, skills monitoring, job moves, promotions and staff re-structuring.
- *To Monitor Work-Related Licenses and Credentials*, including provisioning licenses for use in the course of an employee's work-related responsibilities, ensuring compliance, training, examination and other requirements are met with applicable regulatory bodies.
- *To Provide Our Employees with Human Resources Management Services*, including providing employee data maintenance and support services, administration of separation of employment, approvals and authorization procedures, administration and handling of employee claims, and travel administration.
- *To Maintain Your Contact Information*, including altering your details across relevant entities within PDS affiliated entities (for example personal, other employment and transferring roles).
- *To Assist You in Case of Emergency*, including maintenance of contact details for you, and your dependents in case of personal or business emergency.
- *To Monitor Eligibility to Work in the U.S.*, which means monitoring and ensuring compliance of employees' ability to work in the U.S.
- *To Conduct Healthcare-Related Services*, including conducting pre-employment and employment-related medical screenings for return-to-work processes and medical case management needs; determining medical suitability for particular tasks; identifying health needs of employees to plan and provide appropriate services, including operation of sickness policies and procedures.

- *To Facilitate Better Working Environment*, which includes conducting staff surveys, providing senior management information about other employees, and conducting training.
- *To Ensure a Safe and Efficient Working Environment*, which includes PDS actions relating to disciplinary actions, and code of conduct processes and investigations.
- *To Maintain Security on PDS Websites and Internet Connected Assets*, which includes hosting and maintenance of computer systems and infrastructure; management of PDS's software and hardware computer assets; systems testing, such as development of new systems and end-user testing of computer systems; training; and monitoring email and Internet access.
- *To Comply with Applicable Law or Regulatory Requirements,* such as legal (state and federal) and internal company reporting obligations, including headcount by ethnicity and gender, management information, demographic and health, safety, security and environmental reporting.
- *For other employment and HR purposes, such as assessing a job applicant's credentials and work experience*.

Any information collected is disclosed to you here and is used as permitted or required by law.

6. Disclosure of Personal Information

We may disclose personal information to any of the entities identified as sources of personal information. We may also disclose any personal information to the following:

- **Customers**. We disclose personal contact information to customers as part of the normal customer service relationship.
- **Company Affiliates**. We disclose personal information about our workforce members to other entities affiliated with the Company, including our parent and subsidiary companies.
- **Legally Required Parties.** Persons to whom we are required by law to provide information, such as pursuant to a subpoena or a court order.
- **Reorganization Recipients.** Persons involved in the consideration, negotiation, completion of a business transaction, including the sale, merger, consolidation, acquisition, change in control, transfer of substantial assets, bankruptcy, or reorganization, and any subsequent integration.
- **Authorized Recipients:** To any party when authorized by the individual to whom it pertains to share it.

7. Data Retention

We retain personal information for various periods depending on the nature of the personal information, the purposes for its collection and use, and based on our legal and ethical obligations. Generally, we retain personal information only for so long as necessary to fulfill the purposes for which we collected it. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information; the potential risk of harm from unauthorized use or disclosure of your personal information; the purposes for which we process your personal information and whether we can achieve those purposes through other means; and the applicable legal requirements.

8. Your California Privacy Rights

California Residents have certain rights under the CCPA. For information on how to exercise these rights, please see below.

- **The Right to Know.** The right to know what personal information the Company has collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about you.

- **The Right to Deletion**. The right to delete personal information that the business has collected about you, subject to certain exceptions.

- **The Right to Correction**. The right to correct inaccurate personal information that a business maintains about a California resident.

- **The Right to Opt-Out of the Sale/Sharing**. If we sell or share personal information, the right to opt-out of the sale or sharing of your personal information by the Company.

- **The Right to Limit the Use of Sensitive Personal Information**. If the Company uses or discloses sensitive personal information for reasons other than those permitted by the CCPA, the right to limit the use or disclosure of sensitive personal information by the Company.

- **Non-Discrimination**. The right not to be discriminated against for exercising any of the rights conferred by the CCPA.

The Company will honor the privacy rights afforded to individuals in accordance with applicable law.

Exercising Your CCPA Rights

Workforce Members who are California residents may submit CCPA requests themselves or using an authorized agent. CCPA requests are subject to our verification measures which vary depending on the type of request made and the sensitivity of the information you request. We may ask you to provide a few pieces of information to confirm your identity in our records. If you authorize an agent to submit a request on your behalf, we may require the agent to provide proof that you gave the agent signed permission to submit the request and may verify the agent's identity and authority to act on your behalf.

- **Submitting Access, Deletion, and Correction Requests**

To make a right to know (access), deletion, or correction request, please submit a CCPA request form or call our dedicated toll-free CCPA request phone number at 888-508-2033.

- **Limiting the Use of Your Sensitive Personal Information**

Californian's have the right to limit a business's use or disclosure of sensitive personal information. However, the Company does not use or disclose sensitive personal information for any purpose other than for permissible purposes under the CCPA. Therefore, we do not offer a mechanism to submit these requests.

- **Opting Out of the Sale/Share of Your Personal Information**

The Company does not sell or share personal information related to the workforce member relationship. Please review the privacy policies located on our Company websites for more information about opt-out rights for website visitors.

9. How Do I Contact PDS Health with Questions About the California Employee and Applicant Privacy Notice?

If you have any questions about this Privacy Notice, please email us at: privacy@pacden.com.