



Acelpa Health – California Privacy Policy

Last Updated July 22, 2025.

Acelpa Health, LLC and its affiliates and subsidiaries, (“we,” “our,” or “us”) owns and operates the website found at www.acelpahealth.com, other websites, our mobile applications and other services that link to this California Privacy Policy (this “Policy”) or the General Privacy Policy (collectively, the “Services”). Pursuant to the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”), Acelpa Health provides the following Policy regarding the categories of personal information that we collect, use, and disclose about California residents (“you”, “your”). This Policy only applies to California consumers and supplements the information contained in our General Privacy Policy, which is incorporated herein.

Under the CCPA, “personal information” is information that identifies, relates to, or could reasonably be linked with a particular California resident or household. “Personal information” does not include any publicly available, deidentified, aggregated or anonymized information.

Personal Information We Collect, Use, or Disclose

Under the CCPA, we disclose the following information regarding our collection, use, and disclosure of your personal information. The following chart describes the categories of personal information that we collected about consumers in the last 12 months. For each category, if applicable, we have identified the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties and service providers with whom we disclose personal information.

Business or commercial purposes are defined as follows:

- ❑ **Auditing and Ad Impressions:** Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- ❑ **Security and Fraud Detection:** We use personal information for our security and fraud detection services including: detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for that activity.
- ❑ **Functionality & Debugging:** to identify and repair errors that impair existing intended functionality.
- ❑ **Services on Our Behalf:** including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information,



processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

- ❑ **Internal Research and Development:** We use personal information for our internal research related to technological development and demonstration.
- ❑ **Marketing and Services:** We use personal information to provide advertising or marketing services on our own behalf.
- ❑ **Audits:** We use personal information to audit current interactions with you and related transactions (e.g., counting and verifying ad impressions, auditing compliance).
- ❑ **Legal Obligations:** We use and disclose your identifiable health information when we are required to do so by federal, state, or local law.

Categories of Personal Information	The Categories of Sources From Which the Personal Information is Collected	The Business or Commercial Purpose(s) for Which the Information is Collected, Used, and/or Shared	Third parties to whom Disclosed for Business Purpose
Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, or other similar identifiers.	<ul style="list-style-type: none">❑ Directly from You❑ Cookies on our Services❑ Service Providers❑ Web and Data Analytics Service Providers❑ Financial and Payment Technology Providers❑ Identity Verification Services	<ul style="list-style-type: none">❑ Auditing and Ad Impressions❑ Security and Fraud Detection❑ Functionality & Debugging❑ Services on Our Behalf❑ Internal Research · Legal Obligations❑ Advertising and Marketing Services❑ Audits	<ul style="list-style-type: none">❑ Data Analytics Service Providers❑ Our Service Providers

Categories of Personal Information	The Categories of Sources From Which the Personal Information is Collected	The Business or Commercial Purpose(s) for Which the Information is Collected, Used, and/or Shared	Third parties to whom Disclosed for Business Purpose
Internet or other similar network activity. This may include browsing history, search history, or information on a consumer's interaction with a website, application, or advertisement.	<input type="checkbox"/> Directly from You <input type="checkbox"/> Cookies on our Services <input type="checkbox"/> Service Providers <input type="checkbox"/> Web and Data Analytics Service Providers	<input type="checkbox"/> Auditing and Ad Impressions <input type="checkbox"/> Security and Fraud Detection <input type="checkbox"/> Functionality & Debugging <input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Internal Research <input type="checkbox"/> Legal Obligations <input type="checkbox"/> Advertising and Marketing Services Audits	<input type="checkbox"/> Data Analytics Service Providers <input type="checkbox"/> Our Service Providers
Characteristics of protected classifications under California or federal law, such as age and medical conditions;	<input type="checkbox"/> Directly from You <input type="checkbox"/> Service Providers	<input type="checkbox"/> Auditing and Ad Impressions <input type="checkbox"/> Security and Fraud Detection <input type="checkbox"/> Functionality & Debugging <input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Internal Research <input type="checkbox"/> Advertising and Marketing Services Audits	<input type="checkbox"/> Data Analytics Service Providers <input type="checkbox"/> Our Service Providers
Commercial information, such as transaction information and purchase history	<input type="checkbox"/> Directly from You <input type="checkbox"/> Service Providers	<input type="checkbox"/> Security and Fraud Detection <input type="checkbox"/> Functionality & Debugging <input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Internal Research <input type="checkbox"/> Advertising and Marketing Services Audits	<input type="checkbox"/> Our Service Providers
Geolocation data, such as device location;	<input type="checkbox"/> Directly from You <input type="checkbox"/> Cookies on our Services	<input type="checkbox"/> Security and Fraud Detection <input type="checkbox"/> Functionality & Debugging <input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Internal Research <input type="checkbox"/> Advertising and Marketing Services Audits	<input type="checkbox"/> Our Service Providers

Categories of Personal Information	The Categories of Sources From Which the Personal Information is Collected	The Business or Commercial Purpose(s) for Which the Information is Collected, Used, and/or Shared	Third parties to whom Disclosed for Business Purpose
Audio, electronic, visual and similar information, such as call and video recordings;	<input type="checkbox"/> Directly from You	<input type="checkbox"/> Security and Fraud Detection <input type="checkbox"/> Functionality & Debugging <input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Internal Research <input type="checkbox"/> Advertising and Marketing Services Audits	<input type="checkbox"/> Our Service Providers
Professional or employment-related information; and this may include current or past job history or performance evaluations.	<input type="checkbox"/> Directly from You <input type="checkbox"/> Our Service Providers	<input type="checkbox"/> Services on Our Behalf <input type="checkbox"/> Legal Obligations <input type="checkbox"/> Audits	<input type="checkbox"/> Our Service Providers
Sensitive personal information including biometric information. This may include physiological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish your identity	<input type="checkbox"/> You	<input type="checkbox"/> Internal Research	<input type="checkbox"/> n/a

Acelpa Health uses sensitive personal information solely for the purposes that you would anticipate in providing us the information.

Categories of Parties To Whom We May Disclose Your Personal Information

- ☐ Our employees, contractors, and/or related entities;
- ☐ Our existing or potential agents or business partners;
- ☐ Courts, tribunals, regulatory authorities, and law enforcement officers, as required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise, or defend our legal rights;
- ☐ Software and service providers we use to manage and process your information, for example, customer service providers.
- ☐ Marketing service providers we use to communicate with you.
- ☐ Advertising service providers we use to assist us in providing personalized advertising on third party websites
- ☐ Financial and payment technology providers.
- ☐ Background check companies.
- ☐ Identity verification services.

If we receive personal information about you from a third party, we will protect it as set out in this Policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such person's consent to provide the personal information to us.

Security of Your Personal Information

When we collect and process personal information, and while we retain this information, we will protect it within commercially acceptable means to prevent loss and theft, as well as unauthorized access, disclosure, copying, use, or modification. Although we will strive to use commercially acceptable means to protect the personal information you provide to us, we advise that no method of electronic transmission or storage is 100% secure, and no one can guarantee absolute data security. We will comply with laws applicable to us in respect of any data breach. You are responsible for selecting any password and its overall security strength, ensuring the security of your own information within the bounds of our services.

How Long We Keep Your Personal Information

We keep your personal information only for as long as we need to for each disclosed purpose. This time period may depend on what we are using your information for, in accordance with this Policy. If your personal information is no longer required, we will delete it or make it anonymous by removing all details that identify you. However, if necessary, we may retain your personal information for our compliance with a legal, accounting, or reporting obligation or for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes.

Your Rights Under California Law

If you are a California resident, you may exercise certain privacy rights related to your personal information. We may limit our response to your exercise of these privacy rights as permitted under



applicable law. You may submit your request using our toll-free number, via email or via [online form](#). If you make a request to exercise one of your privacy rights via e-mail, please include "Privacy Rights Request" in the subject line of the email. The rights of California residents are:

- ❑ **The Right to Know/Access:** You have the right to request that Acelpa Health disclose what personal information it collects, uses, discloses, and sells. This is called the "Right to Know". Under the Right to Know, you can request a listing of the types of personal information we have collected about you, the sources of that information, how we use the information (e.g., our business or commercial purposes for collecting or selling personal information), other individuals and business with whom we share personal information, and the specific pieces of personal information that we have collected about you.
- ❑ **The Right to Correct:** You have the right to request that we correct inaccurate personal information we maintain about you. You may review the personal information we have collected about you as described in The Right to Know/Access, above.
- ❑ **The Right to Delete:** You have the right to request that we delete your personal information, subject to certain limited exceptions.
- ❑ **The Right to Opt-Out of the Sale or Sharing on Personal Information:** We may use analytics and advertising technologies, including those provided by advertising partners that use your Personal Information to serve you targeted advertising that is based on your activity across our Services and third-party websites, apps and services. While we do not disclose your Personal Information for money, these activities may be considered "sales," under the CCPA. You have the right to opt-out of the sale of and/or cross-context behavioral advertising uses of your personal information by Acelpa Health. To opt-out, click [here](#), or download and use a browser supporting the Global Privacy Control (GPC) browser signal. If you choose to use the GPC signal, you will need to turn it on for each browser you use.
- ❑ **The Right to Non-Discrimination:** We will not discriminate against you for exercising any of your rights over your personal information.

Verification of Your Identity

As required or permitted under applicable law, we may take steps to verify your request before providing personal information to you, deleting personal information, or otherwise processing your request. To verify your request, you must provide your name, email address, phone number, and state of residence. If we believe we need further information to verify your request as required



by law, we may ask you to provide additional information to us. We will review each request carefully and respond accordingly within the timeframe established by the CCPA. If necessary, we may need additional time to respond where allowed by law, but we will reply either way within the legally required period and, if we need an extension, we will explain why. In certain cases, a request may be denied, for example, if we are required to keep a record of services you have purchased in order to comply with tax reporting requirements. If we deny your request, we will explain why we denied it.

Authorized Agents.

You may designate an authorized agent to make a request on your behalf. We will deny requests from agents that do not submit proof of authorization from you. To verify that an authorized agent has authority to act for you, we may require a copy of a power of attorney or require that you provide the authorized agent with written permission and verify your own identity with us.

"SHINE THE LIGHT" LAW

Under California Civil Code Section 1798.83, California residents with whom we have an established business relationship are entitled to request and receive, free of charge, once per calendar year, information about the personal information we shared, if any, with other businesses for their own direct marketing uses during the prior year.

You can make such a request by contacting us. Please include "Shine the Light Inquiry" in your email subject line if you contact us by email.

Children

Acelpa Health does not knowingly collect personal information from children under the age of 16, and users under the age of 16 should not submit any personal information to Acelpa Health. If Acelpa Health has actual knowledge that personal information about a child under 16 years old has been collected, then Acelpa Health will take the appropriate steps to delete this personal information.

Limits of Our Policy

Our Services may link to external sites that are not operated by us. Please be aware that we have no control over the content and policies of those sites and cannot accept responsibility or liability for their respective privacy practices.

Changes to This Policy

At our discretion, we may change this California Privacy Policy to reflect updates to our business processes, current acceptable practices, or legislative or regulatory changes. If we decide to



change this Policy, we will post the changes here at the same link by which you are accessing this Policy.

Contact Us

For any questions or concerns regarding your privacy, you may contact us using the following details:

Mail: 12110 Hadley Street, Whittier, CA 90601

Attn: Corporate Compliance

Email: privacy@acelpahealth.com

Phone: (877) 602-7779

California Workforce and Applicant Privacy Notice.

This section (the "California Workforce and Applicant Privacy Notice") applies to our current and former employees or individual independent contractors ("Workforce Members") and job applicants, ("Applicants"), who are California residents when the CCPA covers our collection and use of your Personal Information in the employment context.

This California Workforce and Applicant Privacy Notice does not apply to our collection and use of Personal Information in a consumer or business-to-business capacity or to Personal Information collected about Workforce Members and Applicants who are not California residents.

Workforce Member and Applicant Personal Information We Collect and Disclose.

The following chart provides information about the types of Personal Information that we have collected from California Workforce Members and Applicants, the purposes for which we used the information, and the categories of third parties with whom we have shared this information in the last 12 months.

Type of Information	Business Purpose	Categories of Third-Party Recipients
Identifiers: real name, alias, postal address, Social Security number, driver's license number, passport number, email address or other similar identifiers	<ul style="list-style-type: none">• Establish, manage, terminate or otherwise administer the employment relationship• To verify employment eligibility• To monitor and provide compensation, payroll, tax, and	<ul style="list-style-type: none">• Third party service providers who provide employment related services, such as recruiting, human resource, payroll and benefits providers

	<p>benefits planning, enrollment, and administration</p> <ul style="list-style-type: none"> • To manage Workforce Member performance • For Workforce Member development, education and training • To comply with laws and regulations, including, without limitation, applicable tax, health and safety, anti-discrimination, immigration, labor and employment laws • To monitor, investigate, and enforce compliance with and potential breaches of our policies and procedures and legal and regulatory requirements • To comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons • To exercise or defend the legal rights of us and our Workforce Members, affiliates, customers, contractors, and agents. 	
<p>Internet or other electronic network activity information: browsing history, search history,</p>	<ul style="list-style-type: none"> • To manage Workforce Member performance • To monitor, maintain, and secure company 	<ul style="list-style-type: none"> • Third party service providers

information regarding an individual's interaction with our services, software and emails, and electronic communication metadata.	systems, networks, databases, equipment, and facilities	
Geolocation data: IP addresses and Device location	<ul style="list-style-type: none"> To manage Workforce Member performance To monitor, maintain, and secure company systems, networks, databases, equipment, and facilities To monitor, investigate, and enforce compliance with and potential breaches of our policies and procedures and legal and regulatory requirements 	<ul style="list-style-type: none"> Third party service providers
Professional or employment-related information: Current or past job history or performance evaluations	<ul style="list-style-type: none"> Establish, manage, terminate or otherwise administer the employment relationship To verify employment eligibility To manage Workforce Member performance For Workforce Member development, education and training To comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons 	<ul style="list-style-type: none"> Third party service providers

	<ul style="list-style-type: none"> To exercise or defend the legal rights of us and our Workforce Members, affiliates, customers, contractors, and agents. 	
Non-public education information: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	<ul style="list-style-type: none"> Establish, manage, terminate or otherwise administer the employment relationship To verify employment eligibility To manage Workforce Member performance For Workforce Member development, education and training 	<ul style="list-style-type: none"> Third party service providers
Sensitive Personal Information: Social Security number, driver's license, state identification card, passport number; precise geolocation; consumer's racial or ethnic origin, citizenship or immigration status	<ul style="list-style-type: none"> Establish, manage, terminate or otherwise administer the employment relationship To verify employment eligibility To monitor and provide compensation, payroll, tax, and benefits planning, enrollment, and administration To manage Workforce Member performance To comply with laws and regulations, including, without limitation, applicable tax, health and safety, 	<ul style="list-style-type: none"> Third party service providers

	anti-discrimination, immigration, labor and employment laws	
--	---	--

We obtain the categories of Personal Information listed above from the following categories of sources:

- Directly from you, such as from the forms you fill out or information you input into our HR system.
- Indirectly from you, such as from your interactions with Acelpa Health's computer systems and applications.
- From our service providers, such as recruiting partners, HR management providers, background check providers, and internet service providers.
- From other employees, such as from performance reviews or other observations and interactions.

Retention of Workforce Member and Applicant Personal Information.

We will retain California Workforce Member and Applicant Personal Information for the period reasonably necessary to perform the employment-related purposes described above and for the purpose of satisfying any legal, accounting, contractual, or reporting requirements that apply to us.

Your Rights.

If you are a California Workforce Member or Applicant, you have the rights described in the Your Rights Under California Law section, above. We will not discriminate against you for exercising any of these rights.

Exercising Your Rights.

California Workforce Members and Applicants may exercise their rights by contacting us using one of the methods described in the Contact Us section above.

You may designate an authorized agent to make a request on your behalf. We will deny requests from agents that do not submit proof of authorization from you. To verify that an authorized agent has authority to act for you, we may require a copy of a power of attorney or require that you provide the authorized agent with written permission and verify your own identity with us.