

FinThrive Privacy Notice for California Residents

Last Updated: December 29, 2022

This **Privacy Notice for California Residents** (“Notice”) supplements the information contained in the Company’s general Privacy Policy (available on our website) and applies solely to those consumers who **reside in the State of California** (“consumers” or “you”).

This Notice is intended to provide specific information to consumers in California and to describe your rights related to your personal information. We adopt this Notice to comply with the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), and its implementing regulations and any terms defined in the CCPA/CPRA have the same meaning when used in this Notice.

This Notice does not include personal information collected by FinThrive as part of an **employee–employer relationship**, including **applicants and candidates for employment** with FinThrive. FinThrive maintains separate notices for our use of personal information in these instances. Job applicants and candidates for employment can view the relevant notice on our Privacy Resources page.

Information We Collect

The Company collects information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household (**personal information**). The Company collects and uses personal information generally for our business purposes, to provide the services for which you have inquired or purchased, and to be in legal compliance.

In particular, the Company has collected or disclosed the following categories of personal information about its consumers within the last twelve (12) months:

Category	Examples	Collected	Sold or Shared	Disclosed for a Business Purpose	To whom we disclosed personal information
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, passport number, or other similar identifiers.	YES	NO	YES	Service Providers (For example, consultants, website developers, IT providers, auditors)
B. Personal information categories listed in the California Customer	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card	YES	NO	YES	Service Providers

Records statute (Cal. Civ. Code § 1798.80(e)).	number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.					(For example, consultants, website developers, IT providers, auditors)
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO	NO	NO		Not Applicable
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO	NO	NO		Not Applicable
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO	NO	NO		Not Applicable
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES	NO	YES		Service Providers (For example, consultants, website developers, IT providers, auditors)
G. Geolocation data.	Physical location or movements.	YES	NO	YES		Service Providers (For example, consultants,

					website developers, IT providers)
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO	NO	NO	Not Applicable
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO	NO	NO	Not Applicable
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	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.	NO	NO	NO	Not Applicable
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO	NO	NO	Not Applicable
L. Sensitive Personal Information	A social security, driver's license, state identification card, or passport number.	NO	NO	NO	Not Applicable
	Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	YES	NO	YES	Service Providers (For example, IT providers, contracted staff)
	Precise geolocation or any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.	NO	NO	NO	Not Applicable
	Racial or ethnic origin, religious or philosophical beliefs, or union membership.	NO	NO	NO	Not Applicable
	The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.	NO	NO	NO	Not Applicable

Genetic data	NO	NO	NO	Not Applicable
The processing of biometric information for the purpose of uniquely identifying a consumer.	NO	NO	NO	Not Applicable
Personal information collected and analyzed concerning a consumer's health.	NO	NO	NO	Not Applicable
Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.	NO	NO	NO	Not Applicable

Personal information **does not** include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA/CPRA's scope, like:
 - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
 - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994 (DPPA).

Use of Personal Information

We may use the personal information collected about you for the following purposes:

- To provide, administer and communicate with you about our technology solutions, services, events, surveys and promotions (including by sending you marketing communications) or to market our solutions (e.g. your customer references or testimonials, provided only with your consent).
- To facilitate and personalize your experience with our Sites and/or technology solutions and to administer those Sites and technology solutions.
- To determine and manage the effectiveness of our advertising and marketing, for example by engaging in surveys or research to understand our customer-base, conduct analysis of product adoption, evaluate customer success and user behaviors within our solutions.
- To enable you to do business with us, for example, by conducting sales meetings, customer implementation projects, vendor onboarding, contracting processes, or related administrative activities for our customer and vendor management.
- To process, evaluate and respond to your requests, inquiries, or support cases.
- To evaluate, grow and improve our business (including activities such as developing new products and services, enhancing current products or services, market research, quality

assessment and improvement activities, cost studies, data aggregation and analytics, customer reference program, advisory councils, etc.).

- To carry out or obligations and enforce our rights arising from any contracts entered into between us and you.
- To protect and secure our Sites, technology solutions, data, assets, network, and business operations, and to detect, investigate, and prevent activities that may violate our policies or be fraudulent or illegal.
- To comply with legal process, such as warrants, subpoenas, court orders, and lawful regulatory or law enforcement requests and to comply with legal, regulatory compliance, or contractual obligations
- To conduct general business operations such as accounting, recordkeeping, compliance activities and audits
- To defend the interests of the Company or employees in threatened or actual legal proceedings, investigations or inquiries.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by FinThrive is among the assets transferred.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA/CPRA.

The Company only collects or processes your sensitive personal information for the purposes expressly permitted by the CCPA/CPRA and its implementing regulations. The Company does not collect or process sensitive personal information for the purpose of inferring characteristics about you.

The Company will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sources of personal information

The Company obtains the categories of personal information listed above from the following categories of sources which are described more fully in our Privacy Policy:

- Directly from you. For example, information you provide via a form on our website or when creating a user account in one of our technology solutions.
- Indirectly from you. For example, from logging your actions in our technology solutions or through cookies stored in your browser and similar technologies.
- From our Service Providers, for example information obtained through IT service providers or marketing consultants.
- From courts or government agencies, for example information received regarding a court subpoena.

Disclosure of Personal information

The Company may disclose your personal information to external parties for a business purpose, including those noted above. When we disclose personal information for a business purpose to a Service Provider or Contractor, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

We also may disclose your personal information to other third parties when required by law or to meet a legal or compliance obligation.

We disclose your personal information to the following categories of external parties:

- Service providers who are providing a service for, or on behalf of, the Company such as information technology partners, contractors provided by staffing agencies, auditors, accountants, marketing consultants.
- In the case of customer reference data, testimonials or other customer stories related to our solutions, to other customers or prospective customers, but only with prior consent from you.
- Relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings).
- As required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, meet a compliance obligation or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

Sale or Sharing of Personal Information

The Company does not sell personal information or share personal information for cross-text behavioral advertising.

Retention of Personal Information

The Company maintains a Records Retention Policy that outlines our practices for retention of business-related information. We are subject to certain legal and regulatory requirements to retain certain information for a defined period of time. Absent a specific requirement to retain personal information based on the retention schedule, a contractual or regulatory obligation, litigation hold or other legitimate business purpose, the Company deletes information (including each category listed above) when it is no longer necessary for the proper operation of the Company.

Your Rights and Choices

The CCPA, as amended by the CPRA, provides consumers (California residents) with specific rights regarding their personal information. This section describes your rights and explains how to exercise those rights.

Your Right to Know and Access Specific Pieces of Personal Information

You have the right to request that the Company disclose certain information to you about our collection and use of your personal information. Once we receive and confirm your verifiable consumer request (see Exercising Access, Deletion, and Correction Rights), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting, selling, or sharing that personal information.
- The categories of third parties with whom we disclose that personal information.
- The specific pieces of personal information we collected about you (if requested, also called a Data Portability request).
- If we sold or shared your personal information, or disclosed it for a business purpose, two separate lists disclosing:
 - The categories of personal information sold or shared about you and the categories of third parties to whom the information was sold or shared (by category of personal information for each category of third party); and
 - The categories of personal information disclosed about you for a business purpose and the categories of persons to whom it was disclosed.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. Your request for access or data portability will apply to personal information collected on or after January 1, 2022, that is still maintained by the Company at the time of the request. You may specify a shorter time-period for your request at your option.

Your Right to Delete Personal Information

You have the right to request that the Company delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, Deletion, and Correction Rights), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.

- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Your Right to Correct Inaccurate Personal Information

You have the right to request that the Company correct inaccurate personal information that we maintain about you. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, Deletion, and Correction Rights), we will use commercially reasonable efforts to correct (and direct our service providers to correct) your inaccurate personal information in our records.

Exercising Access, Data Portability, Deletion and Correction Rights

To exercise the access, data portability, deletion, and correction rights described above, please submit a verifiable consumer request via email to privacy@finthrive.com or by calling us toll-free at 1-877-636-5442.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you choose to designate an authorized agent to make a request on your behalf, you must provide us with written authorization or a power of attorney, signed by you, for the agent to act on your behalf. You will still need to verify your identity directly with us such as through an email address we have on file.

The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative. If you are making a request from a personal email, we may need to verify your address or other information to validate against our system information. Authorized representatives may be asked to provide documentation to support their role.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

For instructions on exercising sale opt-out rights, see *Your Right to Opt-Out of Personal Information Sale or Sharing*.

Response timing and format

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. The response we provide will explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Your Right to Opt-Out of Personal Information Sale or Sharing

The Company does not sell or share personal information described in this Notice. However, if you are 16 years of age or older, you have the right to direct us to not sell or share your personal information at any time (the "right to opt-out"). We will maintain your preference on file to prevent any future sale or sharing.

We do not sell or share the personal information of consumers we actually know are less than 16 years of age, unless we receive affirmative authorization (the "right to opt-in") from either the consumer who is between 13 and 16 years of age, or the parent or guardian of a consumer less than 13 years of age. Consumers who opt-in to personal information sales may opt-out of future sales at any time.

To exercise the right to opt-out, you (or your authorized representative) may submit a request via email to privacy@finthrive.com or by calling us toll free at 1-877-636-5442.

Once you make an opt-out request, we will wait at least twelve (12) months before asking you to reauthorize personal information sales. However, you may change your mind and opt back in to personal information sales at any time by submitting a request to privacy@finthrive.com or by calling 1-877-636-5442.

You do not need to create an account with us to exercise your opt-out rights. We will only use personal information provided in an opt-out request to review and comply with the request.

Your Right to Limit the Use and Disclosure of Sensitive Personal Information

You have the right to request that the Company limit its use of your sensitive personal information when used for purposes other than those permitted by the CCPA/CPRA and its implementing regulations. Sensitive personal information that is collected or processed as permitted is not subject to this “Right to Limit” and is treated as personal information (and thus subject to other rights listed above). The Company only collects or processes your sensitive personal information for the purposes expressly permitted by the CCPA/CPRA and its implementing regulations.

Your Right to No Retaliation

You have the right to exercise your rights without retaliation. We will not discriminate against you for exercising any of your CCPA/CPRA rights. Unless permitted by the law, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

If you feel that you have experienced retaliation, you are encouraged to call the Company’s Helpline at 1-844-680-0572.

However, we may offer you certain financial incentives permitted by the CCPA that **can result** in different prices, rates, or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information’s value and contain written terms that describe the program’s material aspects. Participation in a financial incentive program requires your prior opt in consent, which you may revoke at any time.

California Shine the Light

California’s “Shine the Light” law (Civil Code Section §1798.83) permits California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, submit your request to privacy@finthrive.com. Please allow 30 days for a response.

Notice of Sale of De-Identified Information

With appropriate authorizations, FinThrive may sell or disclose deidentified information derived from patient information which is not subject to the CCPA/CPRA. Such information is de-

identified in accordance with Section 164.514(b)(1) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method.

Changes to Our Privacy Notice

The Company reserves the right to amend this Notice at our discretion and at any time. When we make changes to this Notice, we will post the updated notice on our Website and update the Notice's "last updated" date.

Contact Information

If you have any questions or comments about this Notice, the ways in which the Company collects and uses your information described in this Notice, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at privacy@finthrive.com.