

Agiliti Inc.

Privacy Notice for California Residents

The California Privacy Rights Act of 2020 (“CPRA”) as of January 1, 2023 requires certain entities to provide additional privacy-related information to residents of California.

This **Privacy Notice for California Residents**, on behalf of Agiliti Inc. and all subsidiaries (“Agiliti,” “us,” “our” or “we”), supplements the information contained in our general **Privacy Notice** which can be found by clicking on the **PRIVACY & DATA COLLECTION NOTICES** link in the website footer. This **Privacy Notice for California Residents** applies solely to all visitors, users, and others who reside in the State of California (“consumers” or “you”). This Privacy Notice for California Residents is intended to describe our privacy practices and rights for those who 1) use Agiliti’s websites or URLs controlled or operated by Agiliti which link to this policy (“Websites”) or services, or 2) otherwise provide us with information through various means. We adopt this notice to comply with the CPRA and any terms defined in the CPRA have the same meaning when used in this Notice.

EXEMPTIONS AND EXCLUSIONS FROM THIS POLICY ARE: The following are not covered by or are otherwise exempt by law from this **Privacy Notice for California Residents**.

- Personal information collected outside of California.
- Household data
- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Health or medical information covered by the California Confidentiality of Medical Information Act (CMIA) which can include information received under other California laws such as the California Family Rights Act, California’s Pregnancy Disability Leave law and the federal Family Medical Leave Act, clinical trial data, or other qualifying research data.
- Protected Health Information (PHI) collected by covered entities (CEs) or business associates (BAs) governed by the privacy, security, and breach notification rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (“HIPAA exemption”) (Cal. Civ. Code §§ 1798.145(c)(1)(A), (B) and 1798.146(a)(1)). The CPRA’s HIPAA exemption applies to an individual’s PHI that is accessed, created, or maintained in relation to employer-sponsored group health plans (which are HIPAA CEs). Group health plans include insured and self-funded major medical health plans, dental and vision plans, health reimbursement arrangements (HRAs), and health flexible spending arrangements (health FSAs).
- Protections for trade secrets
- Protections for free speech and press rights for noncommercial activities protected by California’s Constitution.

Information We Collect

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer,

household, or device ("**personal information**"). As noted above in the Exemptions and Exclusions section, this **Privacy Notice for California Residents** does not apply to certain personal information.

The table below displays the categories of personal information we collect or have collected from California consumers within the last twelve (12) months. For a detailed disclosure related to California Workforce personal information collection and purposes see our **CPRA Notice at Collection for California Employees and Applicants** located by first clicking on the **PRIVACY & DATA COLLECTION NOTICES** link in our website footer, and then clicking the link for California Residents.

We have also identified in the table below types of **sensitive personal information** we collect. Sensitive personal information is a subtype of personal information, and because we do not collect or use this information to infer characteristics about a person and we only use this sensitive personal information for the purposes stated in this notice, the CPRA does not treat this information as sensitive and for that reason we have described within our personal information categories.

Category of Personal Information (including sensitive personal information)	Examples of Information We Collect	Collected
A. Identifiers.	First and last 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, marital status, facsimile number, and date of birth.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, 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.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, 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 may be collected by Agiliti's health insurance provider), veteran or military status, genetic information (including familial genetic information may be collected by Agiliti's health insurance provider).	YES

Category of Personal Information (including sensitive personal information)	Examples of Information We Collect	Collected
D. Commercial information.	Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories, survey responses.	YES
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.	YES
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website (cookies), application, or advertisement.	YES
G. Geolocation data.	Physical location or movements of Agiliti drivers.	YES
H. Sensory data.	Audio, electronic, visual, thermal, or similar information.	YES
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
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
K. Inferences drawn from other personal information.	Preferences for Agiliti products of interest to you.	YES
L. Sensitive Personal Information:		
(1) Government Identifiers	(1) First and last 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, marital status, facsimile number, and date of birth.	(1) Yes
(2) Complete account access credentials	(2) user names, account numbers, or card numbers combined with required access/security code or password	(2) Yes

Category of Personal Information (including sensitive personal information)	Examples of Information We Collect	Collected
(3) Precise geolocation	(3) Physical access to a Company office location, Physical location or movements of Agiliti drivers in the field.	(3) Yes
(4) Racial or ethnic origin	(4)	(4) Yes
(5) Religious or philosophical beliefs	(5) Review and process religious reasonable accommodation requests for example related to COVID 19 vaccination requirements	(5) Yes
(6) Union membership	(6)	(6) No
(7) Mail, email, or text messages content not directed to us	(7)	(7) Yes
(8) Genetic data	(8)	(8) Yes
(9) Unique biometric information used for identification	(9) Fingerprints for certain licensing and registration requirements	(9) Yes
(10) Health information	(10) Job restrictions and workplace illness and injury information	(10) Yes
(11) Sex life, or sexual orientation information	(11)	(11) No

How we collect information

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete or products and services you purchase.
- Indirectly from you. For example, from observing your actions on our Websites. Visit our Cookie Notice for more information on the types of cookies we use on our Websites.
- From third parties. For example, potential job candidates from talent agencies.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to request a price quote or ask a question about our products or services,

we will use that personal information to respond to your inquiry. If you provide your personal information to purchase a product or service, we will use that information to process your payment and facilitate delivery. We may also save your information to facilitate new product orders or process returns.

- To provide, support, personalize, and develop our Websites, products, and services.
- For business operations, including for marketing purposes.
- To create, maintain, customize, and secure your account with us.
- To facilitate recruiting endeavors and human resources administration.
- To process your requests, purchases, transactions, and payments and prevent transactional fraud.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your experience on our Websites and to deliver content and product and service offerings relevant to your interests.
- To help maintain the safety, security, and integrity of our Websites, products and services, databases and other technology assets, and business.
- To interact with auditors, regulators, legislators, or other public servants or government agencies.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CPRA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.

We 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.

How long do we keep your Personal Information

We store your personal information (including sensitive personal information) for different time periods depending on the category of personal information and in accordance with applicable accounting and record retention laws. We strive to keep personal information for no longer than as needed to achieve the purpose for which it is collected and to comply with applicable accounting and record retention laws. To determine how long we will retain your personal information we consider a number of factors like the category, how the personal information relates to our need to provide the services to you, and what our legal and accounting obligations are to retain the personal information.

Sharing Personal Information

We do not use cross-context behavioral advertising. We do not sell your personal information. We may share your personal information with service providers, contractors, lawyers, auditors, consultants, or other third parties for a business purpose, as required by law, with your consent, or for verification purposes in connection with a CPRA request. In the preceding twelve (12) months, we have disclosed personal information for a business purpose to the categories of third parties as listed below.

- Identifiers: to Internet Cookie Data Recipients; and service providers for payroll and benefits
- California Customer Records: to service providers for payroll and benefits
- Protected classification characteristics: to our health insurance provider
- Commercial Information: to payment processors
- Internet or other similar network activity: to our website host and Internet Cookie Data Recipients
- Geolocation data: to our fleet management vendor
- Professional Employment Related Information: to service providers of payroll and benefits

Consumers have the right to opt-out of a covered business' sale of their personal information and the right to direct us to stop sharing your personal information for cross-context behavioral advertising. We do not sell personal information to any third-party and we do not use cross-context behavioral advertising. In the preceding twelve (12) months, we have not sold personal information or used cross-context behavioral advertising.

Protection of Personal Information

While we cannot guarantee absolute security, we use reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification or disclosure.

Your Rights and Choices

The CPRA provides consumers (California residents) with specific rights regarding their personal information and sensitive personal information. This section describes your CPRA rights and explains how to exercise those rights.

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection, use, and disclosure of your personal information collected in the past 12 months (the "right to know"). Once we receive your request and confirm your identity (see Exercising Your 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 or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
 - sales, identifying the personal information categories that each category of recipient purchased; and
 - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

- The specific pieces of personal information we collected about you (also called a data portability request).

Right to Delete

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions (the "right to delete"). Once we receive your request and confirm your identity (see Exercising Your Rights), we will review your request to see if an exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. 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, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
6. 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.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify personal information not subject to one of these exceptions from our records and will direct our service providers and contractors to take similar action.

Right to Correct

You have the right to ask us to correct inaccurate personal information about you. Once we receive your request and confirm your identity (see Exercising Your Rights), we will use commercially reasonable efforts to correct the inaccurate personal information as directed by you.

Exercising Your Rights

Only you, or someone legally authorized to act on your behalf, may make a request to know, delete or correct related to your personal information. Your Request to Know, Delete or Correct must describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it. You may only submit a request twice within a 12-month period.

Communication Methods

To exercise your rights to know, delete or correct described above, please submit a request by any of the following Communication Methods:

- Clicking on the **PRIVACY & DATA COLLECTION NOTICES** link in the website footer, then clicking on the CALIFORNIA RESIDENTS link, then clicking on PRIVACY REQUEST FORM.
- Emailing us at privacyofficer@agilitihealth.com;
- Postal mail at Agiliti Health, Inc., Attention: Privacy Officer, 11095 Viking Drive, Suite 300, Eden Prairie, MN 55344
- Calling us at 1-800-847-7368.

You do not need to create an account with us to submit a request to know, delete or correct.

How Your Identity will be Verified

For your privacy and security, and to prevent fraud and other harmful activities, when we receive a request through one of the Communication Methods, we need to ensure that the person submitting the request is the person they purport to be. Accordingly, we will take reasonable measures to verify the identity of the person making the request. We ask you to provide personal information to help us verify your identity, but we will use that information only for the purpose of verification; we will not use the additional personal information you provide for any other purpose. Initially, we ask you to provide basic personal information when you submit a request. This information will include your first name, last name, email address, address, and telephone number. Providing accurate information that matches our records is necessary so that we can locate the correct information within our systems and among our service providers.

Your request to know, delete or correct must provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information and verify the identity of an authorized representative, if applicable. The degree of proof required, and the type of information necessary to prove your identity, will vary depending upon the nature of the request and the sensitivity of the information.

For example, for requests to know the categories of personal information collected and used about you, or to delete non-sensitive information with a low risk of harm, we will verify your identity to a reasonable degree of certainty, usually by matching at least two data points you provide with information we have.

For requests of specific pieces of personal information about you, we will verify your identity to a reasonably high degree of certainty, usually by matching three or more data points provided by you to data points we have on record, as well as collecting a signed declaration under penalty of perjury stating you are the person to which the request relates.

Requests from an Authorized Agent

To designate an authorized agent, the authorized agent must furnish evidence of your identity (the subject of the request), must furnish evidence of the agent's identity, and must provide evidence that he or she is your authorized agent. To provide evidence that the agent is authorized to act on your behalf, the agent may either provide a Power-of-Attorney, or signed permission by you for the agent to act on your behalf, or you may directly confirm with us that you provide consent for the agent to make the request.

Requests from a Parent or Guardian

We do not knowingly collect personal information from children under the age of 16. If you are under the age of 16, you should not provide any personal information to us. If you are a parent or guardian of a child under the age of 16 and suspect they have provided personal information to us, you may contact us using one of the Communication Methods described above.

Only a parent or legal guardian can make requests to know, delete or correct personal information about a consumer under age 13. You may make a request to know, delete or correct on behalf of your child under age 13 subject to our verification that you are the child's parent or guardian. To verify that you are the child's parent or guardian, we require that you provide a signed consent form under penalty of perjury stating that you are the child's parent or guardian and that you consent to the request. Such request should be returned to us via postal mail, email or our web form listed under the Communication Methods above and meet the other request requirements outlined above.

Other Verification Methods

To prove your identity, we may ask you to provide:

- a copy of a government-issued identification (with driver's license, passport number, or other identification number redacted prior to submission); or
- a signed declaration under penalty of perjury.

We may also conduct verification through a third-party identity-verification service.

If we ask you to verify your identity, you must promptly cooperate with our efforts so that we can fulfill your request. If you do not comply, your request cannot be fulfilled.

Response Timing and Format

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10 business day timeframe, please send an email to privacyofficer@agilitihealth.com.

We endeavor to substantively respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding our receipt of your request. The response we provide will also 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.

Non-Discrimination

You have the right to not receive discriminatory treatment by a covered business for exercising your CPRA consumer rights. We will not discriminate against you for exercising any of your CPRA rights. This right does not prohibit us from offering loyalty, rewards, premium features, discounts or club card program nor prohibits us from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to us by your data. Unless permitted by the CPRA, 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.
- Retaliate against an employee, applicant for employment, or independent contractor for exercising their rights under this title.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on the Websites and update the notice's effective date. **Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.**

Contact Information

If you have any questions or comments about this notice, the ways in which Agiliti collects and uses your information described here or in the general **Privacy 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:

Phone: 1-800-847-7368

Email: privacyofficer@agilitihealth.com

Postal Address:

Agiliti Health, Inc.
Attn: Privacy Officer
11095 Viking Drive, Suite 300
Eden Prairie, MN 55344

If you need to access this Policy in an alternative format due to having a disability, please contact privacyofficer@agilitihealth.com or 1-800-847-7368.

Document No.: DP002 vr 081423

Effective Date: August 24, 2023

Last Updated On: August 14, 2023