

Kentra Health California Privacy Notice

Effective Date: 12/27/2025

Last Updated on: 12/27/2025

This California Privacy Notice describes how Kentra Health and its subsidiaries, affiliates, and related entities (collectively, "Kentra Health," "Kentra Health," "we," or "us") collect and process personal information about our consumers who reside in California. The California Consumer Privacy Act ("CCPA") requires us to provide our California consumers with a privacy policy that contains a comprehensive description of our online and offline practices regarding our collection, use, sale, sharing, and retention of their personal information, along with a description of the rights they have regarding their personal information. This Privacy Policy provides the information the CCPA requires, together with other useful information regarding our collection and use of personal information. Any terms defined in the CCPA have the same meaning when used in this policy.

This Privacy Policy does not apply to our collection and use of personal information from residents outside of California. Consumers residing in other locations should see our general privacy policy at: <https://assets.kentrahealth.com/documents/privacy-notice.pdf>.

Personal Information Collected

We collect and use 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 or household ("**personal information**"). Personal information does **not** include:

- Publicly available information, including from government records, through widely distributed media, or that the consumer made publicly available without restricting it to a specific audience.
- Lawfully obtained, truthful information that is a matter of public concern.
- Deidentified or aggregated consumer information.

Personal Information Categories Chart

The chart below identifies the categories of personal information we collected from our consumers within the last 12 months.

Category	Examples	Collected
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

B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) (" California Customer Records ").	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, 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.	YES
C. Protected classification characteristics under California or federal law (" Protected Classes ").	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, reproductive health decision-making, military and veteran status, or genetic information (including familial genetic information).	YES/
D. Commercial information.	Records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	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.	Activity on our websites, mobile apps, or other digital systems, such as internet browsing history, search history, system usage, electronic communications with us, postings on our social media sites.	YES
G. Geolocation data.	Physical location or movements	NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information	NO

I. Professional or employment-related information.	Current or past job history.	NO
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)) (" FERPA 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.	NO
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO
L. Sensitive personal information.	Further identified in the chart below.	YES

We retain personal information for as long as necessary to carry out the purposes for which we originally collected it and for other purposes described in this Notice and our Privacy Policy <https://assets.kentrahealth.com/documents/privacy-notice.pdf>.

Sensitive Personal Information Categories Chart

Sensitive personal information is a subtype of personal information consisting of the specific information categories listed in the chart below. Importantly, the CCPA only treats this information as sensitive personal information when we collect or use it to infer characteristics about a consumer.

The chart below identifies which sensitive personal information categories, if any, we have collected from consumers to infer characteristics about them in the last 12 months.

Sensitive Personal Information Category	Collected to Infer Characteristics?
L.1. Government identifiers, such as your Social Security number (SSN), driver's license, state identification card, or passport number.	NO

L.2. Complete account access credentials, such as usernames, account logins, account numbers, or card numbers combined with required access/security code or password.	NO
L.3. Precise geolocation, such as GPS data from a consumer's mobile device that can provide its location in a geographic area, with an approximate radius of 1,850 feet.	NO
L.4. Racial or ethnic origin.	YES
L.5. Citizenship or immigration status.	NO
L.6. Religious or philosophical beliefs.	NO
L.7. Union membership.	NO
L.8. Mail, email, or text messages not directed to the Kentra Health.	NO
L.9. Genetic data.	YES
L.10. Neural Data, such as information generated by measuring a consumer's central or peripheral nervous system's activity that is not inferred from nonneural information.	NO
L.11. Unique identifying biometric information.	YES
L.12. Health information.	YES
L.13. Sex life or sexual orientation information.	YES

Sources of Personal Information

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

- Directly from you, such as from the forms or other information you provide to the Kentra Health.
- Indirectly from you, such as from your interactions with the Kentra Health's websites and mobile applications.
- From our service providers, such as data analytics providers.
- Inferences generated by the Kentra Health's or our service providers' computer systems.

Sensitive Personal Information Use and Disclosure Purposes

We may use or disclose sensitive personal information for the following statutorily approved reasons (**Permitted SPI Purposes**):

- Performing actions that are necessary for our consumer relationship and that an average consumer in a relationship with us would reasonably expect.

- Preventing, detecting, and investigating security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
- Defending against and prosecuting those responsible for malicious, deceptive, fraudulent, or illegal actions directed at the Kentra Health.
- Ensuring physical safety.
- Short-term, transient use, such as non-personalized advertising shown as part of your current interactions with us, where we do not:
 - disclose the sensitive personal information to another third party; or
 - use it to build a profile about you or otherwise alter your experience outside your current interaction with the Kentra Health.
- Services performed for the Kentra Health, including maintaining or servicing accounts, processing or fulfilling transactions, verifying consumer information, processing payments, or providing financing, analytic services, storage, or similar services for the Kentra Health.
- Activities required to:
 - verify or maintain the quality or safety of a product, service, or device that we own, manufacture, had manufactured, or control; or
 - improve, upgrade, or enhance the service or device that we own, manufacture, had manufactured, or controlled.
- Collecting or processing sensitive personal information that we do not use for the purpose of inferring characteristics about a consumer.

We do not use or disclose sensitive personal information for purposes other than the Permitted SPI Purposes. For more on your right to limit these additional sensitive personal information use purposes, see [Your Rights and Choices](#).

Additional Categories or Other Purposes

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. If required by law, we will also seek your consent before using your personal information for a new or unrelated purpose.

We may collect, process, and disclose aggregated or deidentified consumer information for any purpose, without restriction. When we collect, process, or disclose aggregated or deidentified consumer information, we will maintain and use it in deidentified form and will not attempt to reidentify the information, except to determine whether our deidentification processes satisfies any applicable legal requirements.

Disclosing, Selling, or Sharing Personal Information

Business Purpose Disclosures

We have not disclosed consumers' personal information to third parties for a business purpose in the preceding 12 months.

Selling or Sharing Personal Information

We do not sell your personal information, including sensitive personal information, to third parties and have not sold it in the preceding 12 months. We do not share your personal information with third parties for cross-context behavioral advertising purposes and have not shared your personal information in the preceding 12 months.

Your Rights and Choices

If you are a California resident, the CCPA grants you the following rights regarding your personal information:

Right to Know and Data Portability Requests

You have the right to request that we disclose certain information to you about our collection and use of your personal information (the "**right to know**"), including the specific pieces of personal information we have collected about you (a "**data portability request**"). You may exercise your right to know **twice** in any 12-month period. Once we receive your request and confirm your identity (see [How to Exercise Your Rights](#)), we will disclose to you:

- The categories of:
 - personal information we collected about you; and
 - sources from which we collected your personal information.
- The business or commercial purpose for collecting your personal information and, if applicable, selling or sharing your personal information.
- If applicable, the categories of persons, including third parties, to whom we disclosed your personal information, including separate disclosures identifying the categories of your personal information that we:
 - disclosed for a business purpose to each category of persons; and
 - sold or shared to each category of third parties.
- When your right to know submission includes a data portability request, a copy of your personal information, subject to any permitted redactions.

Right to Delete and Right to Correct

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 and limitations (the "**right to delete**"). Once we receive your request and confirm your identity, we will delete your personal information from our systems unless an exception allows us to retain it. We will also notify our service providers to take appropriate action.

You also have the right to request correction of personal information we maintain about you that you believe is inaccurate (the "**right to correct**"). We may require you to provide documentation, if needed, to confirm your identity and support your claim that the information is inaccurate. Unless an exception applies, we will correct personal information that our review determines is inaccurate and notify our service providers, contractors, and other recipients to take appropriate action.

Right to Limit Sensitive Personal Information Use and Disclosure to Permitted SPI Purposes

You have a right to ask businesses that use or disclose your sensitive personal information to limit those actions to just the CCPA's Permitted SPI Purposes (the "**right to limit**"). As we do not use or disclose sensitive personal information beyond the CCPA's Permitted SPI Purposes, we do not currently provide this consumer right.

Personal Information Sales or Sharing Opt-Out and Opt-In Rights

You have the right to request that businesses stop selling or sharing your personal information at any time (the "**right to opt-out**"), including through a user-enabled opt-out preference signal. Similarly, the CCPA prohibits businesses from selling or sharing the personal information of consumers it actually knows are under 16 years old without first obtaining consent from consumers who are between 13 and 15 years old or the consumer's parent or guardian for consumers under age 13 (the "**right to opt-in**").

As we do not sell or share consumers' personal data, we do not currently provide these consumer rights.

Right to Non-Discrimination

You have the right not to be discriminated or retaliated against for exercising any of your privacy rights under the CCPA.

How to Exercise Your Rights

Exercising the Rights to Know, Delete, or Correct

To exercise the right to know (including data portability), delete, or correct described above, please submit a verifiable request to us by either:

- Calling us at kenneth@kentrahealth.com.
- Emailing us at kenneth@kentrahealth.com.
- Contact us via email at kenneth@kentrahealth.com.

Please describe your request with sufficient detail so we can properly understand, evaluate, and respond to it. You or your authorized agent may only submit a request to know, including for data portability, twice in a 12-month period.

Verification Process and Authorized Agents

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. We may request specific information from

you or your authorized representative to confirm your or their identity before we can process your right to know, delete, or correct your personal information.

We cannot respond to your request to know, delete, or correct if we cannot verify your identity or authority to make the request and confirm the personal information relating to you. We will only use personal information provided in the request to verify the requestor's identity or authority to make the request.

We consider requests made through your password-protected account with our company sufficiently verified when the request relates to personal information associated with that specific account. You do not need to create an account with us to submit a request to know, correct, or delete.

For requests to limit or opt-out, we ask for the information necessary to complete the request, which may include, for example, the consumer's name, email address, or account username.

Responding to Your Requests to Know, Delete, or Correct

We will confirm receipt of your request within ten business days. If you do not receive confirmation within the ten-day timeframe, please contact us at kenneth@kentrahealth.com.

We endeavor to substantively respond to a verifiable request within 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 to your verified email address or, if you have a password protected account with us, to your account. Our substantive response will tell you whether or not we have complied with your request. If we cannot comply with your request in whole or in part, we will explain the reason, subject to any legal or regulatory restrictions. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, deleted, or made your personal information anonymous in compliance with our record retention policies and obligations.

Any disclosures we provide will cover information for the 12-month period preceding the request's receipt date. We will consider requests to provide a longer disclosure period that do not extend past January 1, 2022, unless providing the longer timeframe would be impossible or involves disproportionate effort.

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 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.

Privacy Policy Changes

We reserve the right to update this Privacy Policy at any time, as we continue to develop our compliance program in response to legal developments of the CCPA. If we make any material changes to this Privacy Policy, we will update the policy's effective date and post the updated policy on our website. We encourage you to check our website to review the current Privacy Policy in effect.