BeyondWell

BeyondWell Health Privacy Policy

Effective Date: September, 2019
Last Updated: March 2025

BeyondWell Health Privacy Policy

BeyondWell Health ("BeyondWell," "we," "our," or "us") is committed to protecting your privacy and ensuring transparency regarding the data we collect, how it is used, and the control you have over your personal information. This Privacy Policy clearly outlines our practices concerning data collection, usage, sharing, security, and retention.

Protections from Disclosure of Medical Information

We are required by law to maintain the privacy and security of your personally identifiable health information ("PHI"). Although the wellness program and your employer may use aggregate information it collects to design a program based on identified health risks in the workplace, BeyondWell will never disclose any of your personal information either publicly or to the employer, except as necessary to respond to a request from you for a reasonable accommodations needed to participate in the wellness program, or as expressly permitted by law. Medical information that personally identifies you that is provided in connection with the wellness program will not be provided to your supervisors or managers and may never be used to make decisions regarding your employment.

Your health information will not be sold, exchanged, transferred, or otherwise disclosed except to the extent permitted by law to carry out specific activities related to the wellness program, and you will not be asked or required to waive the confidentiality of your health information as a condition of participating in the wellness program or receiving an incentive. Anyone who receives your information for purposes of providing you services as part of the wellness program will abide by the same confidentiality requirements. The only individual(s) who will receive your personally identifiable health information is (are) healthcare professionals, such as health coaches, nurses, or other health professionals, in order to provide you with those services, should you receive them, under the wellness program.

In addition, all medical information obtained through the wellness program will be maintained separate from your personnel records, information stored electronically will be encrypted, and no information you provide as part of the wellness program will be used in making any employment decision.

You may not be discriminated against in employment because of the medical information you provide as part of participating in the wellness program, nor may you be subjected to retaliation if you choose not to participate.

Types of Data Collected

BeyondWell collects the following types of data:

- Personal information (e.g., name, email address, phone number, and health-related information)
- Usage and activity data (e.g., how you interact with our app, pages visited, cookies)
- Device and technical information (e.g., IP address, device type, operating system)

How We Use Your Data

We use your data for the following purposes:

- Providing, improving, and personalizing our services
- Analyzing user interaction to enhance user experience
- Communicating important updates, changes, or support information
- Ensuring compliance with applicable laws and regulations

Data Sharing and Disclosure

We do not sell your personal information. Data may be shared with:

- Service providers and partners that support the functionality and operation of our services
- Regulatory authorities, if legally required or necessary to protect our rights and those of others

Data Security and Protection

Protecting your personal information is important to us. We are committed to protecting the information you provide through the Platform. We attempt to protect online information according to applicable laws and established company security standards and practices. BeyondWell implements robust security measures, including encryption, secure data storage, and restricted access to safeguard your personal information against unauthorized access,

disclosure, or misuse. However, we cannot guarantee the confidentiality or security of electronic transmissions via the Internet because they may potentially use unsecure computers and links, and data may be lost or intercepted by unauthorized parties during such transmission. If you wish to submit personal or confidential information by a more secure means of communication, contact us.

Data Retention and Deletion Policy

We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required by law. Upon your request, we will securely delete or anonymize your personal information.

User Rights and Opt-Out Options

You have the right to:

- Access your personal data
- Request correction or deletion of your data
- Withdraw consent or opt-out of specific data collection practices

You may exercise these rights by contacting us through our designated privacy contact below.

Privacy Contact

For privacy inquiries, questions, or requests related to your personal data, please contact us at:

BeyondWell Privacy Compliance Team
Email: compliance@cambiahealth.com
Toll-Free: 877-878-2273

Cookies, Pixels & Similar Technologies

Technologies like cookies, pixels and other identifiers (collectively, "Cookies and Similar Technologies") are used to deliver, secure and understand products and services that we offer. Cookies are small files that are placed on your browser or device by the website you are viewing or app you are using. Pixel tags (also called clear GIFs, web beacons or pixels) are small blocks of code on a website or app that allow them to do things like read and place cookies and transmit information to us.

We use Cookies and Similar Technologies for a variety of reasons, such as allowing us to show you content and material that's most relevant to you, improving our products and services, and helping to keep our products and services secure. While specific names of the Cookies and Similar Technologies that we use may change from time to time as we improve and update our products and services, they generally fall into the following categories of use: authentication, security, insights and measurements, localization, and Platform features and performance.

We sometimes use Infrastructure Vendors or partner with Third Party Partners to help us provide or inform you of certain products and services that are benefits offered through your group health plan. We may contract with these other companies that use Cookies and Similar Technology to collect information regarding your interaction with the Platform or your use of both the Platform and Third Party Websites and Partners. We may transfer information to Infrastructure Vendors who support our business, such as providing technical infrastructure services, storing, hosting or transferring data, analyzing how our products and services are used, measuring the effectiveness of services, providing customer service, and facilitating payments, incentives, or rewards. We may also transfer information to Third Party Partners who offer you additional services or features through our Platform.

Most browsers will allow you to disable cookies, can be set to notify you when you receive a cookie and thus give you an option to not accept it, or will allow you to choose an option not to have the browser track you. If you choose to disable cookies, certain functionality of a website or the Platform may be impaired or not work at all.

More Information

Device data

You agree that we, our Infrastructure Vendors, or our Third Party Partners may collect the following information periodically and without further notice to you as a result of your use of the Platform: technical data and related

information, including but not limited to technical information about your device, system and application software, and peripherals.

Third parties

The Platform may provide links to other websites that are not owned or controlled by BeyondWell ("Third Party Websites"). BeyondWell has no control over other websites or other resources accessed through such links. BeyondWell provides links to Third Party Websites to connect you to additional sources of health information or Third Party Services that may be of interest to you. Such links are provided for your convenience only, and do not constitute an endorsement of the Third Party Websites or content by BeyondWell. BeyondWell makes no guarantees and disclaims any implied representations or warranties about the accuracy, relevance, timeliness, completeness or appropriateness of these third-party resources, the information contained in them or the products or services they provide. BeyondWell shall not be liable, directly or indirectly, for any damage or loss incurred by you in connection with websites or resources accessed through links. We may also provide access to services managed by Third Party Partners with whom we have made arrangements to offer you these services through the App. These Third Party Partners may be co-branded, meaning that they display the our logo and the logo of the Third Party Partner, or white-labeled, meaning that they display just the our name and/or logo, but they are owned and controlled by the Third Party Partner. In each such instance, where practicable, we will let you know when you are leaving the App and accessing a Third Party Partner. The Third Party Partners may collect data you submit to provide you with access to their service; to understand how you use their services; to troubleshoot and protect against errors; to perform data analysis and testing; and to improve their products, among other possible uses. Some of the services made available through the App may be subject to additional Third Party Partner terms, privacy policies, and disclosures, and those terms, privacy policies, and disclosures are incorporated into these Terms by reference, including the following Third Party Partner terms, privacy policies, and disclosures:

- OnLife Privacy Policies

We make no guarantees and disclaims any implied representations or warranties about the accuracy, relevance, timeliness, completeness, or appropriateness of the Third Party Websites or Partners, the information contained in them or the products, or services they provide. We shall not be liable, directly or indirectly, for any damage or loss incurred by you in connection with Third Party Websites accessed through links or the services of Third Party Partners. We are not responsible for the content, security, or the privacy practices of Third Party Websites or Third Party Partners. Review the privacy statement and any terms of use of each Third Party Website you visit or Third Party Partners you access.

Compliance with COPPA

The Platform is not directed at children under the age of 13. BeyondWell complies with the Children's Online Privacy Protection Act and does not knowingly permit registration or submission of personally identifiable information by anyone younger than 13 years of age.

Geographic restrictions

We are based in the state of Oregon in the United States. The Site and the App, including Third Party Partner services, are provided for use only by persons located in the United States. We make no claims that the Site or the App is accessible or appropriate outside of the United States. Access to the Site or App may not be legal by certain persons or in certain countries. If you access the Site or the App from outside the United States, you do so on your own initiative and are responsible for compliance with local laws.

Online Privacy

For more information about privacy or about how BeyondWell generally manages your personal information, see your Group Health Plan or Group Health Plan Administrator's privacy policy.

Effective Date: September 1, 2019

California Citizen Rights

Individuals who reside in the state of California, a "consumer," as that term is defined under California law, have additional rights reserved under the California Consumer Privacy Act (CCPA) and the California Shine the Light law:

- Right to Opt-Out. We do not sell personal information.
- Right to Request Personal Information. As a consumer, you have the “right to know” and request that we disclose what personal information we collect, use, and disclose. See the instructions below for submitting a verifiable request, including through the online request form offered by us. You have the right to request the categories of personal information, as detailed under the CCPA, we have collected and store about you. In addition, you have the right to request categories of sources of personal information we collected about you, the business or commercial purpose for collecting, the categories of third parties with whom we share that personal information, and the specific pieces of personal information we have collected about you. Categories of personal information that we disclosed about you for a business purpose may also be requested, with the appropriate lists provided under the CCPA. Upon receipt of a verifiable consumer request, described below in this Privacy Statement/Notice, from you to access personal information, we will promptly take steps to disclose and deliver, free of charge to you, the personal information required by this section and within the timeframes permitted for responding to exercise of this or other applicable right(s). The information may be delivered by mail or electronically, dependent on portability and technical considerations under the CCPA. We may provide personal information to you at any time following a verified request, but shall not be required to provide personal information to you more than twice in a 12-month period.
- Right to Delete Personal Information. You have the right to request we delete personal information we, or our service providers, store about you. Please keep in mind our response to such a request, upon verification, may include an explanation of the business purpose under which we may retain your information (for example, we would need to retain copies of a business transaction for financial records) in accordance with the CCPA.
- Non-Discrimination. If you elect to exercise any right(s) under this section of our Privacy Statement, we will not discriminate or retaliate against you.

If you are a California consumer and have additional questions based on this section of our Privacy Statement, please use this **web form**, email us at compliance@cambiahealth.com, or call us toll-free at 877-878-2273. Also, be sure to check this policy for updates as we will review it at least every 12 months and make updates as necessary.

Identify Verification Requirement

We are required by law to verify that any data access request submitted under the authority of the CCPA was made by someone with the legal right to access the personal information requested. Therefore, prior to accessing or divulging any information pursuant to a data subject access request, under the terms of the CCPA, we may request that you provide us with additional information in order for us to verify your identity, your request, and legal authority (ex. authorized representative). Only you, or a person registered with the California Secretary of State that you authorize 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. Please indicate in your request if either of these apply, as additional verification may apply (ex. verify consumer’s identify and confirm with impacted person(s) that the authorized agent has permission to submit the request).

A 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. A verifiable request must also include sufficient detail that allows us to properly understand, evaluate, and respond to it.

In general, our verification process includes reviewing the information submitted in the request, comparing it to the right(s) requested; the number of verification points/methods required by the CCPA; and the type, sensitivity, and risk of information requested, including to the consumer, from unauthorized disclosure or deletion. An account is not required with us in order to make a request. We will use personal information provided in a verifiable consumer request to verify the requestor's identity and authority to make the request, or otherwise as permitted by the CCPA

(ex. record retention). We will respond to a verifiable consumer request within 45 days of its receipt, and if we require more time (up to 90 total days), we will inform you of the reason of the extension in writing. A response to a consumer request will be provided as required by the CCPA, such as through an account (if one exists), or otherwise by mail or electronically.

Access Request Responses

Under the CCPA, there may be certain circumstances where we would deny your request to access, receive, or delete personal information we hold. For example, we would deny requests where any such access or disclosure would interfere with our regulatory or legal obligations, where we cannot verify your identity, and/or where exemptions/exceptions permitted by the CCPA apply. We also have the ability under the CCPA to deny requests if it would result in our disproportionate cost or effort. Further, certain rights granted by the CCPA will not be effective until January 1, 2021. However, even where we will not substantively complete a request made under the CCPA, we will still provide a response and explanation to your request within a reasonable time frame and as required by law.

Disclosure of Categories

As defined by the CCPA, categories of personal information collected from consumers by us within the past 12 months include:

Categories	Examples	Collected (Yes or No)
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)).	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.	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).	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, face prints, 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, application, or advertisement.	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 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.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes

Personal information may also be collected in the course of a natural person acting as a current or former job applicant, employee, director, officer, or contractor within the context of that natural person's role. Additional information collected may include emergency contact and information to administer benefits, including to another person.

"Personal information" does not include publicly available information, meaning information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. "Personal information" also does not include consumer information that is deidentified or aggregate consumer information. This Notice addresses online and offline practices by us. Information excluded from the CCPA's scope includes health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Other information excluded includes those covered by the California Confidentiality of Medical Information Act (CMIA) or clinical trial data, and personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Personal information is collected and may be used to provide the services to you, to perform obligations under agreements, to provide information and notifications to you or an authorized representative, to protect the rights and safety of you and/or others, to comply with court and other legal requirements, for business purposes and as otherwise set forth in the CCPA, to conduct organizational and operational needs, and as otherwise described when collecting personal information or within this page. A request for personal information collected and/or deletion, noted above, may involve categories and/or specific pieces of information. However, certain exemptions and exceptions may apply in responding to a request.
This business has not sold categories of personal information within the meaning of the CCPA, including minors under 16 years of age.
Categories of personal information from our consumers disclosed for a business purpose within the past 12 months include:

(A) Identifiers such as real name, alias, postal address, unique identifiers, online identifiers, internet protocol address, email address, account name, social security number, driver's license number, passport number, or similar identifiers;
(B) Categories of personal information as described in California Civil Code 1798.80(e);
(C) Characteristics of protected classifications under California or federal law;
(D) Commercial information, including records of personal property, products or services purchased, obtain, or considered, or other purchasing or consuming histories or tendencies;
(E) Biometric information;
(F) Internet or other electronic network activity information, including but not limited to, browsing history,

search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
(I) Professional or employment-related information; and
(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Business purposes may include auditing (ex. auditing and legal/regulatory compliance), security (ex. detecting security breaches), debugging (ex. identifying and fixing technical errors), short-term uses (ex. ad customization), performing services (ex. processing transactions), internal research (ex. product development), and testing/improvement (ex. improvement of technology).

Categories of sources from which personal information was directly and indirectly collected in the past 12 months include from you and/or authorized agents (ex. documents provided to us related to the services for which you/they engage us, and information we collect in the course of providing services to you/them); interaction with our platforms and services (ex. website portal); and third parties (ex. those that provide services such as purchased information, advertising networks, internet service providers, operating systems and platforms, social networks, and data brokers). This could include information obtained on websites and services from third parties that interact with us in connection with the services we perform or are linked to.

Categories of third parties with whom the business shared personal information in the past 12 months include authorized agents, affiliates, service providers (such as those described previously), contractors, and authorized third parties.

Annual reporting

As required by the CCPA, for the prior calendar year the following information is provided. Number of Requests to Know that we received (13), complied with in whole (0) or in part (0), and denied (13). Number of Requests to Delete that we received (3), complied with in whole (0) or in part (0), and denied (3). Number of Requests to Opt-Out that we received (0), complied with in whole (0) or in part (0), and denied (0). The mean number of days within which we substantively responded to Requests to Know (3.62 calendar days), Requests to Delete (6 calendar days), and Requests to Opt-out (N/A calendar days).

Finally, you may be able to request information contained in the California Citizen Rights section in another language where we provide such notices in the ordinary course of business or in an alternative format if you have a disability. Please see our contact information contained within our Privacy Policy above or below.

Year: 2023

	Request To Know	Request To Delete	Request to Opt Out	Average days to respond
Denied	13	3	0	3.62
Complied in part	0	0	0	N/A
Complied in whole	0	0	0	N/A
Total	13	3	0	
Average days to respond	3.62	6	N/A	0

Contact Us

To make a request please contact us at please contact the us at compliance@cambiahealth.com with "CCPA Personal Information Request" in the subject line, and provide us with full details in relation to your request, including your contact information, the specific name of this business, and any other detail you feel is relevant. You can also use the other contact methods mentioned previously. If you are from another area (ex. state) and believe you are entitled to exercise applicable right(s), please use the email address and/or phone number given and include relevant details.

Last Updated: March 28, 2025