Policy Number: 8010 **Version Number:** 4

Policy Name: OLH - California Consumer Privacy Act Privacy Notice (CCPA)

Authoritative Reference: CCPA

Related Policy/Procedure Number: 8006

Created Date: 02/18/2020 **Last Published Date:** 11/21/2022

Revised By: Joseph Weaver **Approved By:** Sebastian Haupt

BACKGROUND

This policy supplements the information contained in the Onlife Health Privacy Policy. Onlife Health adopted this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA") and other California privacy laws.

SCOPE

To California residents who are not members of a health insurer that has a contract with Onlife Health.

POLICY

CALIFORNIA CONSUMER PRIVACY ACT PRIVACY NOTICE

This PRIVACY NOTICE APPLIES ONLY TO CALIFORNIA RESIDENTS WHO ARE NOT MEMBERS OF A HEALTH INSURER THAT HAS A CONTRACT WITH ONLIFE. If you are a member of a Health Insurer that has a contract with Onlife, your information is Protected Health Information ("PHI") that is protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the contracts between Onlife and our client Health Insurer. PHI is excluded from the California Consumer Privacy Act and this Notice does not apply to you. If you do not know whether or not this Notice Applies to you, please contact Onlife at 877.709.0201.

This Notice supplements the information contained in the Onlife Health Privacy Policy. Onlife Health (collectively, At "we," "us," or "our") adopts this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA") and other California privacy laws. This California Consumer Privacy Act Notice ("Notice") applies solely to visitors, users, members, and others who reside in the State of California ("consumers" or "you"), but are NOT members of a Health Insurer that has a contract with Onlife. Any terms defined in the CCPA have the same meaning when used in this notice.

This Notice applies to the Onlife public websites, member portal and mobile applications only. It does not apply when Onlife is acting as a third party partner and providing services on behalf of our client's health and wellness platforms (a "Client Platform"). If you are a user of a Client Platform, please refer to the Client Platform's Notice of Privacy Practices for information about that Client Platform's use and disclosure of personally identifiable information.

Information We Collect

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("personal information"). In particular, we have collected the following categories of personal information from consumers within the last twelve (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)).	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,	YES

	keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	
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 does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, such as:
    - 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.

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

- Directly from our clients or their agents. For example, from enrollment files and other documents that our clients provide to us related to the services for which they engage us.
- Indirectly from our clients or their agents. For example, through information we collect from our clients in the course of providing services to them.
- Directly and indirectly from activity on our Onlife Health website and services.. For example, from submissions through our website portal or website usage details collected automatically.
- From third-parties that interact with us in connection with the services we perform. For example, from fitness trackers where you have initiated a connection between your fitness tracking provider and you account with us.
- Verbal information with the Engagement Center representatives (health assessment)

Use of Personal Information

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

- To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal information in order for us to provide health and wellness services through Onlife Health website and services we will use that information to provide such services to you.
- To provide you with information, products or services that you request from us.
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To improve our website and present its contents to you.
- For testing, research, analysis and product development.
- As necessary or appropriate to protect the rights, property or safety of us, our clients or others.
- 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 CCPA.
- 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.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, 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 the purposes described herein.

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

Category A: Identifiers.
Category B: California Customer Records personal information categories.
Category C: Protected classification characteristics under California or federal law.

Category D: Commercial Information.

Category E: Biometric.

Category F: Internet or other similar network activity.
Category I: Professional or employment-related information.

Category K. Inferences drawn from other personal information.

We may have shared personal information for the following business purposes:

Category	**Examples**	
1. Auditing	• Advertising analytics • Auditing legal and regulatory compliance	YES
2. Security	• Detecting security breaches • Protecting against fraud and malicious activity • Taking action against wrongdoers (e.g. hackers)	NO
3. Debugging	• Identifying and fixing technical errors	NO
4. Short-term uses	• Contextual ad customization that does not involve or contribute to profiling	NO
5. Performing Services	• Account Maintenance • Customer Service • Processing transactions • Marketing	YES
6. Internal Research	○ To develop or demonstrate technology	NO
7. Testing or improvement	○ To verify or maintain the quality and safety of our service	YES

	○ To improve our technology	

We disclose your personal information for a business purpose to the following categories of third parties:

- Our client health plans and employers.
- Our affiliates.
- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

In the preceding twelve (12) months, we have not sold any personal information.

Your Rights and Choices

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

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, 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 personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, two separate lists disclosing:
    - The categories of personal information we collect about you.
    - The categories of information that we disclosed.
    - The categories of third parties to whom we disclosed the personal information.
    - The categories of personal information that we disclose about your for business purposes.

Deletion Request Rights

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. Once we receive and confirm your verifiable consumer request, 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 providers 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, 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 *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.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at 877.709.0201
- Visiting www.onlifehealth.com
- email: support@onlifehealth.com
- By letter: Postal Address:
  Attn: Privacy
  Onlife Health
  169 Madison Avenue
  STE 11959
  New York, NY 10016

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.
You may only make a verifiable consumer request for access or data portability twice within a 12-month period. 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. An authorized representative request form can be found here.
- 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.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within 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. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. 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

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, 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.

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 notify you by email or through a notice on our website homepage.

Contact Information

If you have any questions or comments about this Notice, our Onlife Health Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

- Calling us at 877.709.0201
- Visiting www.onlifehealth.com
- eMail: support@onlifehealth.com
- By letter: Postal Address:
  Attn: Privacy
  Onlife Health
  169 Madison Avenue
  STE 11959
  New York, NY 10016

DEFINITIONS

RESPONSIBILITIES

Disaster Recovery administers disaster recovery and for the Company and is responsible for the development of recovery strategies and solutions, planning, testing, and restoring the Company's critical business applications.

Employees and contingent workforce are individually accountable for stewardship and appropriate use of the information and system assets that they access.

Human Resources provides direction and oversight for employee policies and practices impacting information security, such as background screenings/investigations, hiring, transfers, terminations, and disciplinary policies.

Information Security Governance Council provides oversight of the Information Security Program and ensures adequate management of risk associated with confidentiality, integrity and availability of information for the Company in accordance with its Charter which includes Executive Leadership and receives a bi-annual report of the Information Security Program disposition.

Information Security administers information and system security for the Company on behalf of the CISO and is responsible for the creation, publication, and maintenance of Information Security Policies, Standards and Baselines; Security Awareness and education; Security Consulting; Strategy and Planning; and Risk Assessment.

Information Technology is responsible for establishing and supporting the Enterprise Architecture and for maintaining the Corporate repository of Enterprise Architecture and Standards. Information Technology Division employees and contingent workers are responsible for compliance with Information Security Policy and Security Architecture regarding all technology-related activities, including but not limited to, development and maintenance of application systems, product acquisitions, network / integration activities. The Senior Director of IT Infrastructure Services is also responsible for approving external network connections into the Company network.

Legal Affairs is responsible for approving contract language, including contracts for release (sharing) of information with appropriate external entities.