SUPPLEMENTAL STATE PRIVACY STATEMENT

Last Updated: March 1, 2026

Castlight Health, Inc., including its affiliates and subsidiaries (collectively, "**Castlight**") and Vera Whole Health, Inc., including its affiliates and subsidiaries, as well as the Vera-friendly PCs, (collectively, "**Vera**") ("**it**," "**our**," "**us**," or "**we**") refers to the two (2) national healthcare delivery organizations providing digital healthcare navigation and clinical and advanced primary care services.

This Supplemental State Privacy Statement is applicable to the above-mentioned companies and is specific to your use of Castlight's "**Castlight Platform,**"and Vera's "**My Vera App,**" which is defined as the suite of company offerings (collectively "**Services**"). This statement supplements the privacy rights and choices of members as described in our Privacy Statement.

Capitalized terms used and not otherwise defined in these terms have the meanings given to them in our Privacy Statement.

This Supplemental State Statement (this "**Supplemental Statement**") is intended our Members, who reside in the United States and reside in a state with a comprehensive consumer state privacy law, and as each law is amended and becomes effective, including any regulations thereunder, to be collectively referred to "**State Privacy Law**" (as listed in **Section 6**).

Generally, we assign certain protections over any Personal Information we collect and that is also considered Protected Health Information ("**PHI**") under the Health Insurance Portability & Accountability Act ("**HIPAA**"). As such, certain Personal Information that is considered PHI may be **exempt** under specific State Privacy Laws. To the extent that such Personal Information is not exempt, this Supplemental Statement shall apply. To the extent that any provision in this Supplemental Statement conflicts with a provision of our Privacy Statement, this Supplemental Statement shall govern with respect to consumers, visitors, and others who reside in applicable states.

Table of Contents:

Section 1: Collection of Personal Information

As described in Section 1 our Privacy Statement, we may collect personal information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, to you or a member of your household. For purposes of this Supplemental Statement only, "Personal Information" has the meaning given to it by your respective state.

We may have collected the following categories of personal information directly from you or about you in the last twelve (12) months. We do not necessarily collect all examples of personal information listed in a particular category, nor do we collect all categories of personal information for all consumers.

Category	Examples
Identifiers	Name, contact information, home address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, Social Security number.
Characteristics of protected classes	Age, race, national origin, citizenship, religion, 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.
Internet or other electronic network activity information	Browsing history, search history, interaction with web sites, applications, or advertisements, length of visit and number of page views, click-stream data, locale preferences, your mobile carrier, date and time stamps associated with transactions, and system configuration information.
Geolocation data	Geolocation data, such as device location, to the extent you have configured your device to permit us to collect such information.
Audio, electronic, visual, thermal, olfactory, or similar information	Voice recordings, CCTV, photographs, videos, for example if you consent to participate in a testimonial for our service offerings.
Inferences drawn from any of the information identified above	Inferences drawn to create a profile about, for example, an individual's preferences, characteristics, predispositions, behavior, attitude, or abilities.
Sensitive Personal Information	The processing of biometric information for the purpose of uniquely identifying a consumer, health information.

We generally do not collect commercial information, financial information, professional or employment related information, or education-related information. To the extent that we collect any professional or employment related information, such information will be subject to our Candidate Privacy Policy.

Section 2: Sources of Personal Information

As described in Section 1 our Privacy Statement, the source from which we may collect personal information comes directly from: (i) you when you provide it to us when you register, input health information and wellness goals, and contact us; (ii) your employer and/or employer sponsored health plan; (iii) automatically collected, if you allow cookies or other tracking technologies when you use our website and mobile application; and (iv) Preferred Partners and/or third parties, if you consent to such disclosure.

We collect your personal information for many reasons such as providing the My Vera and/or Castlight Platform to you. The specific business purposes for the collection of your personal information may be to fulfill or meet the reasons for which your information is provided. For example, when you create your account on My Vera or the Castlight Platform, we will collect your name, email address and other personal information to set up your member or user profile. We may also collect your personal information to perform analytics, comply with legal obligations, etc. To learn more about specific reasons why we collect your personal information, please refer to Section 2 our Privacy Statement**.** We will not collect additional categories of personal information or use the personal information we collect for different, unrelated, or incompatible purposes without providing you with notice.

Section 3: Your Rights And Choices

Consumers who are residents of a State Privacy Law (as defined in **Section 6**) have specific rights. Please note that the below rights are not absolute, and we may be entitled to refuse requests, wholly or in part, where exceptions under applicable law apply.

Consumer Rights	
Right To Access	You have the right to access personal information that we may collect or retain about you. If requested, we shall provide you with a copy of your personal information which we collected as permitted by the State Privacy Laws.
Right To Know	You have the right to request the following about your personal information we collected and used about you: • The specific personal information we have collected; • The categories of personal information we have collected; • The categories of sources from which we have collected your personal information; • The business purpose(s) for collecting or sharing your personal information; • The categories of personal information we disclosed for business purposes; and

	• The categories of third parties to whom we disclosed your personal information. **California Civil Code Section 1798.83 permits you to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes.
Right To Opt-Out / Do Not Sell My Personal Information	You have the right to opt-out of sharing your personal information with third parties for some purposes, including sharing that may be defined as a sale under applicable laws. **Please note, that we do not sell your personal information and we don't share it with third parties for cross-context behavioral advertising.** **In the event we show ads, personal information may be sourced from publicly available, de-identified, or aggregated information. In limited circumstances, specific identifiers such as name, location, registration status are shared with service providers when the applicable law allows and a valid business associate agreement has been signed between us and the service provider.
Do Not Share Or Disclose My Sensitive Personal Information	You have the right to limit how your sensitive personal information is disclosed or shared with third parties to only which is necessary for providing our services to you. You may exercise this right before we may use or disclose any of your sensitive personal information (such as health information).
Right to Deletion	In certain circumstances, you have the right to request that we delete any of your personal information that we collect and retain, subject to certain exceptions. Once deleted and, as applicable, we will direct our service providers to delete your personal information from our records, unless an exception applies. We may deny your request to delete your personal information if retaining the information is necessary for us or our service providers, subject to certain exemptions based on your state of residence. Following your request, limited information pertaining to your deletion request will be kept on file to ensure your personal information is not processed at a later date.
Right to Correct (Rectification)	In certain circumstances, you have the right to request correction of any inaccurate personal information. Upon verifying its validity, we may use commercially reasonable efforts to correct your personal information as directed, to the extent possible.
Right To Data Portability	You also have the right to receive your personal information in a structured and commonly used format that can be transferred to another entity.

Right To Non-Discrimination	You are entitled to exercise the rights described above free from discrimination. This means that we will not penalize you for exercising your rights by taking actions. We will not discriminate against you for exercising your right to know, access, deletion or to opt-out of sales.

Section 4: Exercising Your Rights

If you are a resident of a state with a comprehensive State Privacy Law, you may exercise any of your rights as described in this Supplemental Statement and under applicable State Privacy Laws by contacting us by email at privacy@apreehealth.com. We also have a toll-free number: 1-888-722-0483 (for the Castlight Platform) and 1-888-241-1407 (for My Vera).

1. **Identity Verification.** Please note that we will need to confirm your identity (e.g., first and last name, email address, date of birth, and/or employer) and state residency in order to process your request to exercise your rights. In some instances, we may ask you to provide documentation to verify your identity. If this happens, we will reach out to you directly with this request.

2. **Response Timing.** We will make every effort to respond to your request as soon as we receive and triage it, not to exceed thirty (30) days from when you first contacted us, in the manner you initially contacted us by, generally by email or phone. If you have a complex request, certain states allow us up to ninety (90) days to respond. We will still contact you within thirty (30) days from when you contacted us to let you know if we need more time and the reason for the extension.

3. **Response Format.** We intend to respond to you in the same manner by which you contacted us, however any formal correspondence will be written by mail or email. Any request disclosure we provide will cover only the 12-month period preceding 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 usable and should allow you to transmit the information from one entity to another entity.

4. **Fees.** Except as provided for under applicable privacy laws, there is no charge to exercise any of your legal rights. However, if your request(s) is manifestly unfounded, excessive, or repetitive, we may (as permitted under applicable State Privacy Law, charge a reasonable fee taking in account the administrative costs of providing the information or taking the action requested. We will tell you why we made that decision and provide you with a cost estimate before completing your request.

5. **Denials and Appeals.** We may also refuse to act on the request, if we find the request to be manifestly unfounded or excessive. If we decline to take action, we will inform you of our reason for declining to take action and provide instructions for how to appeal the decision. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to your appeal, including a written explanation of the reasons for the decisions. If

the appeal is denied, we will direct you to a way in which you may contact the applicable Attorney General to submit a complaint.

Section 5: Metrics On Your Rights

To keep you informed on your ability to exercise your rights, we are releasing some key metrics to showcase how often our consumers have engaged and how swiftly we respond.

Metrics On Your Rights (from December 2023 — December 2025)					
	Right To Know	**Right To Correct**	**Right to Opt-Out of Sale***	**Right To Delete**	**Right to Data Portability**
Received	0	1	6	76	19
Fulfilled	0	1	N/A	68	14
Denied	0	0	N/A	8	5
Average Response Time	N/A	1 day	2 Days	1 Day	N/A

***Please Note:** Although we may receive requests to opt-out of the sale of Personal Information, we do not sell your Personal Information.

Section 6: Applicable State Privacy Laws

As of February 2026, the following 20 states have enacted State Privacy Laws designed to increase protections for consumers' personal information and provide consumers with specific rights (as described in Section 3) to control their personal information.

As additional privacy laws become effective, we will update this Supplemental Statement on an annual basis.

1. California: The California Privacy Rights Act of 2020 (CPRA), which amends the California Consumer Privacy Act of 2018 (CCPA).
2. Virginia: The Virginia Consumer Data Protection Act (VA CDPA). Effective: January 1, 2023.
3. Colorado: The Colorado Privacy Act (ColoPA). Effective: July 1, 2023
4. Connecticut: The Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CT DPA). Effective: July 1, 2023.
5. Utah: The Utah Consumer Privacy Act (UCPA). Effective: December 31, 2023.
6. Texas: The Texas Data Privacy and Security Act (TDPSA). Effective: July 1, 2024.
7. Florida: The Florida Digital Bill of Rights (FDBR). Effective: July 1, 2024.

8. Oregon: The Oregon Consumer Data Privacy Act (OCDPA). Effective: July 1, 2024.
9. Minnesota: The Minnesota Consumer Data Privacy Act (MNDPA). Effective: July 31, 2025.
10. Montana: The Montana Consumer Data Privacy Act (MCDPA). Effective: October 1, 2024.
11. Iowa: An Act relating to Consumer Data Protection (Iowa CDPA). Effective: January 1, 2025.
12. Delaware's law: The Delaware Personal Data Privacy Act (DPDPA). Effective: January 1, 2025.
13. Nebraska's law: The Nebraska Data Privacy Act (NDPA). Effective: January 1, 2025.
14. New Hampshire: An Act Relative to the Expectation of Privacy (NHPA). Effective: January 1, 2025.
15. New Jersey: An Act Concerning Online Services, Consumers, and Personal Data (NJDPA). Effective: January 15, 2025.
16. Tennessee: The Tennessee Information Protection Act (TIPA). Effective: July 1, 2025.
17. Maryland: The Maryland Online Data Privacy Act (MODPA). Effective: October 1, 2025.
18. Indiana: The Indiana Consumer Data Protection Act, (Indiana CPDA). Effective: January 1, 2026.
19. Kentucky: The Kentucky Consumer Data Protection Act (KCDPA). Effective: January 1, 2026.
20. Rhode Island: Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA). Effective: January 1, 2026.

Version Publication History # ("VPH")

- VPH 1 - January 23, 2025
- VPH 2 - March 1, 2026