

SENECTA CONSUMER HEALTH DATA PRIVACY POLICY

Last updated: 26 August 2026

This Consumer Health Data Privacy Policy is provided separately from our general **Privacy Policy** because the Washington My Health My Data Act, the Nevada consumer health data law (SB 370), and comparable state laws require a distinct policy for consumer health data.

It explains what consumer health data Senecta, Inc. ("**Senecta**", "we", "us") collects, why, who receives it, and how you can exercise your rights. Where this policy and our general Privacy Policy differ on consumer health data, this policy governs.

1. Who this policy is for

This policy is for **residents of homes where a Senecta sensor is installed**, their family members, and anyone else present in such a home, including caregivers and visitors.

Senecta sensors are installed by a care agency in the home of one of its clients. **The care agency decides why the system is installed, who sees the information, and when it is deleted.** Senecta processes that information on the agency's instructions, as a processor and service provider. This is important for exercising your rights, and Section 6 explains what it means in practice.

2. What consumer health data we collect

"Consumer health data" means information that identifies your past, present, or future physical or mental health status. The data Senecta collects that falls into this category is:

Derived health-related insights, which are the outputs the care agency sees:

- changes in daytime and night-time movement patterns
- cough frequency and trends over time
- levels of vocalisation and conversation activity
- bathroom-visit frequency and changes in it
- indications consistent with a fall

The underlying sensor data from which those insights are produced:

- **radar sensing data** showing movement, presence, and position within a room
- **ambient audio**, analysed automatically to detect patterns such as coughing

Senecta sensors contain no camera and capture no images or video.

Ambient audio is analysed automatically by software. No person listens to it: not the care agency, not Senecta personnel, and not any third party. Only the derived insights are made available.

3. Where the data comes from

- directly from Senecta sensors installed in the home
- from the care agency, which provides the residence address and a client reference so the data can be associated with the right household
- generated by our own systems, in the case of the derived insights

We do not buy consumer health data, and we do not obtain it from data brokers or from any source other than those listed above.

4. Why we collect it

We collect and process consumer health data for one purpose: **to provide the monitoring service to the care agency that installed the system**, so that agency can inform the care it delivers to its client.

Specifically, to detect events and generate insights, to deliver alerts and reports to the agency's authorised staff, to support and secure the service, and to comply with our legal obligations.

We also create **de-identified and aggregated** data from it, which we use to improve the service and to train the models behind our detection. De-identified data is not consumer health data, because it can no longer be associated with you. We take reasonable measures to keep it that way, we do not attempt to re-identify it, and we do not use it to contact you or make decisions about you.

We do not use consumer health data for advertising, marketing, or profiling unrelated to care.

5. Who we share it with, and what we never do

The care agency that installed the system, and the staff it authorises. This is the primary and intended recipient.

Service providers who process data on our behalf under written terms that restrict them to our instructions. These fall into five categories: cloud hosting and storage, payment processing, email and application messaging, error monitoring and application telemetry, and product and website analytics. A current list naming each provider is available on request at mauro@senecta.ai.

Legal disclosures, where required by law or to protect the safety of a person.

We do not sell consumer health data. We have never done so. We would not do so without the separate, specific, written authorisation those laws require, which we do not currently seek.

We do not share consumer health data for targeted advertising or cross-context behavioural advertising.

All processing takes place **within the United States**. Our production infrastructure is located in Hillsboro, Oregon.

6. Your rights

You have the right to:

- **confirm** whether we are processing your consumer health data
- **access** that data, including a list of all third parties and affiliates with whom we have shared it, and contact information for each
- **withdraw consent** to its collection and sharing
- **delete** your consumer health data
- **appeal** if we refuse a request
- **not be discriminated against** for exercising any of these rights

How to exercise them. Because the care agency decides what happens with this data, **the fastest route is to contact the agency that installed the system**. They can deactivate and remove the

equipment, and they can instruct us to delete the data.

You can also contact us directly at mauro@senecta.ai, marking your message "Consumer health data request". We will:

- acknowledge your request and verify your identity
- forward it to the relevant care agency and support them in answering it, which is our obligation as a processor
- act on it directly where the law requires us to

We will respond within **forty-five (45) days**, and may extend once by a further forty-five days where the law permits, telling you why.

Withdrawing consent. If you no longer want the system operating in your home, tell the care agency. They are required to deactivate and remove the equipment promptly. Withdrawing consent will not affect your eligibility for care services. You may also tell us, and we will pass it on.

Deletion. Where deletion is requested and required, we will delete the data from our active systems within thirty (30) days and instruct our service providers to do the same. Copies held in backups are deleted on our ordinary backup cycle, within thirty-five (35) days, and are not used for anything in the meantime.

Appeals. If we decline a request, we will explain why and how to appeal. To appeal, reply to our response. We will respond to an appeal within forty-five (45) days. If you remain dissatisfied, you may complain to your state Attorney General. In Washington, that is the Washington State Attorney General's Office.

7. How long we keep it

While a home is active on the service, we keep its history so the system can identify changes over time. That history is what makes the insights meaningful.

When the care agency's agreement with us ends, we delete or return the data within **thirty (30) days**, except where the law requires us to keep it.

8. Security

We maintain administrative, physical, and technical safeguards appropriate to this data, including encryption in transit and at rest, role-based access control with least privilege, and logging of all access. Access is limited to personnel who need it, who are bound by confidentiality obligations and trained on handling consumer health data.

Senecta does not currently hold SOC 2 or ISO 27001 certification and is working toward SOC 2 Type II.

9. Employees and job applicants

This policy does not apply to information Senecta processes about its own employees or job applicants.

10. Changes to this policy

We may update this policy. We will change the date at the top and, where the change is material, give notice before it takes effect. We will not collect, use, share, or sell consumer health data in a way that is materially different from what this policy describes without first obtaining the consent the law requires.

11. Contact

Senecta, Inc.

625 2nd Street, San Francisco, CA 94107, United States

mauro@senecta.ai

Mark privacy requests "Consumer health data request".