REMOTE HOME CHECK, LLC

Privacy Policy

Effective Date: March 1, 2026
Last Updated: March 1, 2026

Remote Home Check, LLC ("RHC," "we," "us," or "our") is committed to protecting the privacy of individuals who use our platform and Services. This Privacy Policy describes how we collect, use, disclose, and safeguard personal information, including health-related data, in connection with the Remote Home Check platform.

This Privacy Policy applies to all users of the Services, including subscribers, monitored individuals, family members, caregivers, and organizational administrators. By using the Services, you consent to the practices described in this Privacy Policy.

This is a dual-track privacy policy covering both HIPAA-regulated data (where a Business Associate Agreement is in effect) and consumer health data regulated under federal and state consumer protection laws.

1. INFORMATION WE COLLECT

1.1 Information You Provide

- Account registration information: name, email address, phone number, mailing address, date of birth
- Payment and billing information: credit/debit card details, billing address (processed by Stripe)
- Profile information for the monitored individual (as provided during onboarding or via connected integrations): name, date of birth, medical conditions, medications, emergency contacts, healthcare providers
- Caregiver assessment inputs: ADL scores, IADL scores, balance test results, memory and cognition assessment responses
- Communications: emails, support requests, and feedback you send to us

1.2 Information Collected Automatically from Devices

The following data is collected passively and non-invasively from integrated devices. No cameras are used.

Apple Watch Data

- Heart rate and heart rate variability; irregular rhythm notifications (as provided by Apple, if enabled by user; RHC does not independently detect or diagnose atrial fibrillation)
- Fall detection events and impact data
- Movement and activity patterns (steps, exercise, standing)
- GPS location data (optional location-based safety signals, if enabled by user; availability depends on device capabilities and user settings)
- Sleep patterns and duration

YoLink Sensor Data

- Bathroom usage patterns (toilet flush frequency and timing via flush sensor)
- Bathroom occupancy and motion patterns (via motion sensor)
- Environmental data from sensor hub

HERO Pill Dispenser Data (PACE Subscribers)

- Medication dispensing events and timing
- Medication adherence rates
- Prescription schedule compliance

Family1st OBD-II Data (Self-Pay Subscribers)

- Driving behavior metrics (speed, braking, acceleration)
- Trip history, routes, and duration
- Vehicle location data

1.3 Information Derived by Our Platform

- Insight Scores: composite wellness scores across physical and mental health domains
- Observations: pattern deviations, trend analyses, and review prompts
- Risk indicators: fall risk, UTI early warning, medication adherence trends, driving risk
- Baseline profiles: individualized normal patterns for each monitored person

1.4 Information from Third Parties

- EMR/EHR data (where integrated with healthcare provider systems under appropriate agreements)
- Monitoring center event records (where Monitoring Center Addendum is active)

2. HOW WE USE YOUR INFORMATION

2.1 Primary Service Purposes

- Providing the Remote Home Check platform and generating Insight Scores and Observations
- Delivering alerts and notifications to designated family members, caregivers, and healthcare professionals
- Processing assessments and updating health domain scores
- Facilitating failover to the UL-certified central station monitoring services (available only when Monitoring Center Addendum (Exhibit G) is executed and active)
- Processing payments and managing subscriptions
- Providing customer support and responding to inquiries

2.2 Platform Improvement

- Improving the accuracy and reliability of our algorithms and detection capabilities
- Developing new features and Services
- Conducting research and analytics using De-Identified and Aggregated Data
- Performing quality assurance and system testing

2.3 Communications

- Sending service-related notifications (alerts, status updates, system maintenance)
- Providing onboarding, training, and educational materials
- Sending account and billing notifications

2.4 Legal and Compliance

- Complying with applicable laws, regulations, and legal processes
- Enforcing our Terms of Service and protecting our rights
- Detecting, preventing, and addressing fraud, security issues, and technical problems

3. HOW WE SHARE YOUR INFORMATION

We do not sell your personal information or Consumer Health Data. We share information only as described below:

3.1 With Your Designated Contacts

Alert data, Insight Scores, and Observations are shared with the family members, caregivers, and healthcare professionals you designate in your account settings.

3.2 With Subprocessors

We share data with our Subprocessors (listed in Exhibit D to the Master Terms of Service and at remotehomecheck.com/legal/subprocessors) solely as necessary to provide the Services. Each Subprocessor is bound by data processing agreements appropriate to the data they handle.

3.3 With Third-Party Device Partners

Data flows to and from Apple (via HealthKit SDK), HERO Health, YoLink, and Family1st as necessary for device integration. Each partner processes data under its own terms of service and privacy policy.

3.4 With Healthcare Providers

Where EMR/EHR integration is active, health data may be shared with the designated healthcare provider systems. This sharing is governed by the applicable BAA or data sharing agreement.

3.5 With the Monitoring Center

Where the Monitoring Center Addendum is active, alert data is shared with the monitoring center partner identified in the applicable Monitoring Center Addendum (Exhibit G) for emergency assessment and dispatch coordination.

3.6 For Legal Purposes

We may disclose information: (a) as required by law, regulation, or legal process; (b) in response to lawful requests by public authorities; (c) to protect the safety of any person; (d) to address fraud, security, or technical issues; or (e) to protect our legal rights.

3.7 In Business Transfers

In the event of a merger, acquisition, or sale of all or a portion of our assets, personal information may be transferred as part of that transaction. We will notify affected users of any such transfer.

4. HIPAA TRACK

This section applies where RHC acts as a Business Associate for a Covered Entity (typically a PACE program or healthcare organization) under an executed Business Associate Agreement (Exhibit H).

4.1 Protected Health Information

When processing PHI on behalf of a Covered Entity, RHC complies with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. PHI is used and disclosed only as permitted by the BAA and HIPAA.

4.2 Individual Rights Under HIPAA

Where HIPAA applies, individuals have the right to:

- Access their PHI maintained by RHC (requests directed through the Covered Entity)
- Request amendment of their PHI
- Request an accounting of disclosures
- Request restrictions on certain uses and disclosures
- Receive confidential communications

4.3 Minimum Necessary Standard

RHC applies the HIPAA minimum necessary standard, limiting the use, disclosure, and request of PHI to the minimum amount necessary to accomplish the intended purpose.

4.4 Breach Notification

In the event of a Breach of Unsecured PHI, RHC will notify the Covered Entity in accordance with the timelines specified in the BAA and applicable law. The Covered Entity is responsible for notifying affected individuals and the Department of Health and Human Services as required.

5. CONSUMER HEALTH DATA TRACK

This section applies to health-related data that is not governed by HIPAA, including data collected from self-pay (B2C) subscribers and data not covered by a BAA.

5.1 FTC Health Breach Notification Rule

RHC complies with the Federal Trade Commission's Health Breach Notification Rule (16 C.F.R. Part 318). In the event of a breach of security involving individually identifiable health information in a personal health record, RHC will notify affected individuals, the FTC, and (where applicable) the media, in accordance with the Rule.

5.2 State Consumer Health Data Laws

RHC complies with applicable state consumer health data protection laws, including but not limited to:

- Washington My Health My Data Act (where applicable to Washington residents)
- California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)
- Connecticut Data Privacy Act
- Other state health data privacy laws as they take effect

5.3 No Sale of Consumer Health Data

RHC does not sell Consumer Health Data. We do not share Consumer Health Data for advertising or marketing purposes of third parties.

5.4 Consumer Rights

Depending on your state of residence, you may have the right to:

- Know what personal information we collect about you
- Access your personal information
- Request deletion of your personal information
- Correct inaccurate personal information
- Opt out of the sale of personal information (we do not sell, but you may exercise this right)
- Withdraw consent for certain processing activities
- Receive a copy of your data in a portable format

To exercise these rights, contact us at privacy@remotehomecheck.com. We will respond within the timeframes required by applicable law (typically 30–45 days).

6. DE-IDENTIFIED AND AGGREGATED DATA

RHC may create De-Identified Data from your information using the HIPAA Safe Harbor method or Expert Determination method. De-Identified Data cannot reasonably be used to identify you. RHC may use De-Identified Data and Aggregated Data for:

- Platform improvement and algorithm training
- Research and analytics
- Industry benchmarking
- Publication of aggregate trends (no individual identification)

De-identification is enabled by default. Organizational customers may opt out via their Order Form. Opting out may reduce the quality of detection algorithms for the opting customer.

7. DATA SECURITY

We implement administrative, physical, and technical safeguards to protect your information, including:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access controls and multi-factor authentication
- Comprehensive audit logging and monitoring
- Multi-tenant data architecture with logical data segregation
- Regular vulnerability scanning and annual penetration testing
- Employee background checks, training, and confidentiality agreements
- Incident response and disaster recovery procedures

For detailed security controls, see the Security Exhibit (Exhibit E) to the Master Terms of Service.

8. DATA RETENTION

We retain your personal information for as long as your account is active or as needed to provide you with the Services. After termination of your subscription:

- Customer Data is available for export for thirty (30) days
- Customer Data is deleted within ninety (90) days after the export period, subject to legal hold or regulatory retention requirements
- De-Identified and Aggregated Data may be retained indefinitely
- Security logs and audit trails are retained for a minimum of one (1) year
- Billing and transaction records are retained as required by applicable tax and financial regulations

9. CHILDREN’S PRIVACY

The Services are not directed to individuals under the age of eighteen (18). We do not knowingly collect personal information from children. If we become aware that we have collected personal information from a child, we will take steps to delete such information.

10. NO CAMERAS

The Remote Home Check platform does not use cameras in any form. All monitoring is passive and non-invasive, using wearable devices (Apple Watch), environmental sensors (YoLink), medication dispensers (HERO), and vehicle monitoring (Family1st). We are committed to preserving the dignity and privacy of the individuals we monitor.

11. THIRD-PARTY LINKS AND SERVICES

The Services may integrate with or link to third-party services (Apple, HERO Health, YoLink, Family1st). These services operate under their own privacy policies. We encourage you to review the privacy policies of any third-party services you use in connection with the Remote Home Check platform. We are not responsible for the privacy practices of third parties.

12. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. Material changes will be communicated by: (a) posting the updated policy on our website at remotehomecheck.com/legal/privacy; (b) updating the “Last Updated” date; and (c) providing notice via email or through the platform at least thirty (30) days before the changes take effect.

Your continued use of the Services after the effective date of any changes constitutes your acceptance of the updated Privacy Policy.

13. CONTACT US

If you have questions about this Privacy Policy, your personal information, or wish to exercise your privacy rights, contact us:

Privacy Inquiries: privacy@remotehomecheck.com
General Support: support@remotehomecheck.com
Legal Notices: legal@remotehomecheck.com

Mailing Address:
Remote Home Check, LLC
Attn: Privacy Officer
200 Briarwood Lane
Canton, GA 30114

[END OF PRIVACY POLICY]