Care Daily Privacy Policy

Version 2.1 | Effective November 4, 2026

This Privacy Policy describes how People Power Company d/b/a Care Daily ("Care Daily," "we") handles personal information through our websites, software, mobile/web experiences, cloud services, partner-branded deployments, connected equipment, customer support, and optional monitoring features. It also covers residents who do not have their own accounts. This Policy does not itself constitute consent, waive legal privacy rights or override a business associate agreement (BAA), data processing addendum (DPA), or other applicable enterprise agreement.

1. Our role depends on who sponsors the Service

When we sell a subscription to a household, we generally determine the purposes and means of the consumer service and act as a business/controller as applicable. When a senior living operator, home-health organization, health plan, insurer, or other client controls a deployment, we may act as its processor/service provider or HIPAA business associate **only under an appropriate separate agreement**. That organization may have its own privacy notice and lawful basis for processing. A reseller may independently control its customer retail relationship and a service-provider partner may act under instructions. We will identify the responsible organization or help a person reach it when a request concerns a customer-controlled deployment.

Preconfiguration and shipment do not authorize continuous household sensing. Device logistics, identity checks, purchase records, and technical provisioning may precede resident authorization; collection or sharing of identifiable household activity or health-related data begins only under a lawful basis and any required notice, consent, or representative authorization.

2. Categories of personal information

Accounts, contact, and relationship details: names, addresses, email, phone, payment token or masked payment details, billing plans, identity/authority evidence, Trusted Circle invitations and access roles, sponsor or reseller association, service period, and support communications.

Household and ambient sensing: installed device identifiers; motion, presence, room activity, door events, button presses, environment, power/connectivity, fall-related signals, sleep/rest indicators and device health. Data may relate to household members, employees, caregivers, and visitors who never create accounts. Depending on enabled hardware, optional integrations may collect voice, video, photos, or other audio/visual content; ordinary ambient-only deployments need not include these features.

Wellness and health-related inferences: activity baselines, mobility/fall-related indicators, sleep patterns, bathroom-visit patterns, wellness/risk scores, caregiver notes, support plans, alerts, escalations, and other generated inferences. These can be sensitive information and consumer health data under state law, even where they are not protected health information under HIPAA.

Device, technical, and website data: connection status, gateway and sensor identifiers, app usage, diagnostics, timestamps, IP addresses, browser type, cookie identifiers, site navigation, crash events, location approximation, and cybersecurity logs.

Communications and monitoring: Trusted Circle messages, emergency-contact and optional call-center instructions, call or notification metadata, service records, and support correspondence. We may process communications content when the related feature is enabled.

Partner-supplied information: approved referrals, agency-sponsored enrollment, care-team contact details, service status, permitted permissions, professional/organizational account data and documented onboarding/authorization records.

3. Information sources

Information comes from individuals and authorized representatives; sponsors, licensed providers, and household administrators; connected devices and integrations; Care Daily platforms; payment, support, marketing, analytics, and security service providers; and communications with us. We may receive information from organizational systems and

electronic health records only where the deployment is separately authorized and supported by required contracts such as a BAA.

4. Why we use it

We process information to provision subscriptions and hardware, verify enrollment authority, operate sensing and alerts, configure care and Trusted Circle permissions, provide requested insights and optional monitoring, handle payments, onboard/support customers, maintain device health, prevent fraud, investigate incidents, comply with law, and maintain secure and reliable services. We may create properly de-identified and aggregated statistics for benchmarking, service quality, research, and product development where legally permitted and contractually authorized. We do not use identifiable consumer health data to train third-party general-purpose AI models without an appropriate lawful basis and required authorization. Care Daily does not sell consumer health data. We do not use health-related inferences for unrelated targeted advertising absent any legally required separate permissions.

Automated analytics may identify patterns, risks, and suggested actions but do not substitute for human decisions about medicine, care, emergency response, housing, employment, or insurance. Any material additional purpose will be disclosed and, where required, separately consented to before use.

5. Sensing without an app; who authorizes it

A device may arrive fully configured. We distinguish shipment and technical readiness from the start of personal sensing and resident data access. For consent-sensitive processing, the resident's valid consent or the decision of an appropriately authorized representative is required where law calls for it. The purchaser, a family member or a provider does not gain automatic authority merely from paying, caring for, or being related to the resident. Where law allows, requests may be explained and recorded in an accessible assisted format, such as an in-person explanation, phone confirmation, or paper authorization. The organization facilitating installation must provide notices to other affected persons as applicable. If a resident objects or disputes authority, we may pause the relevant processing pending review.

Care Daily may hold evidence of notice, representative authority, selected sensor scope, sharing consent, date, version, and accessible method in a consent/authorization record. A person may contact Care Daily without creating an account. Consent may be withdrawn where legally available, though some records may be retained for lawful reasons.

6. Trusted Circle and organizational dashboards

Information may be shared with family, friends, caregivers, service coordinators, professional monitoring providers and an organizational care team **only under the relevant authorization, role, and legal basis**. Permissions can vary, including alerts only, household summaries, care insights, administrative settings, and technical diagnostics. Persons controlling invitations must be authorized to do so; family membership alone is insufficient. Partner dashboards are not a general right to historical resident data, and permissions should be reviewed at discharge, end of sponsorship or change of relationship. We may remove stale access and require verification for sensitive role changes. Information already received by a third party may remain in its own records subject to its legal responsibilities.

7. Optional professional call-center feature

Only activated subscribed Homes are routed to a professional emergency call center. Activation requires the designated subscribed plan, at least two valid emergency contacts, response instructions, and confirmation that the monitoring feature has been enabled. We strongly recommend an end-to-end test and recording its result, but a test is not a universal activation prerequisite unless a specific monitoring plan requires it. The call center may receive limited information necessary to handle the alert, such as contact/location and event information. Not every subscription has this feature; disabling it does not necessarily stop ordinary ambient sensing. A monitoring provider may be an independent controller or service provider depending on its contract and legal obligations, and its specific disclosures will be made available as required.

8. Other disclosures and third-party services

We may disclose information to cloud-hosting and storage providers; customer-support, communications, security, and diagnostic vendors; payment processors; vetted device and integration partners; optional monitoring centers; contractors implementing an authorized Home; the organization's approved staff; trusted individuals authorized by the resident; advisers, financing and acquisition counterparties under confidentiality; and regulators or courts where law requires. Third-party integrations requested by users may be subject to the third party's separate privacy and product

terms. We seek contract protections appropriate to their role and do not make unrestricted disclosures of personally identifiable health information for advertising.

9. Cookies and web technologies

Our websites use essential cookies/technologies for security, load balancing, authentication, and service operation, including infrastructure protections such as Cloudflare. We currently use Google Analytics 4 to understand first-party website engagement, and we may enable embedded Vimeo content when a visitor chooses to play a video. Analytics and media technologies may change; users will receive any legally required notice or choice mechanism. Where Global Privacy Control or another legally recognized opt-out signal applies to a relevant sale, share, or targeted-advertising activity, we honor it as required. We do not use sensitive ambient health data as website advertising segments.

10. Security and retention

We apply reasonable technical, physical, and organizational measures, including access controls, authentication, role limitations, security monitoring, and incident procedures. No system is infallible. We retain personal information for the periods needed to deliver subscribed services, honor permitted care access, satisfy legal/tax/security requirements, prevent fraud, and resolve disputes. Retention depends on data category and customer agreement; when no longer needed, records are deleted, de-identified, or retained as limited backups under a scheduled process. A sponsor's ending relationship does not automatically delete information that must be preserved by law or by an authorized consumer account.

We will provide legally required security or health-data breach notices. Depending on the deployment, laws such as state privacy and breach statutes, HIPAA, and the FTC Health Breach Notification Rule may apply. Business customers and partners must notify us of suspected unauthorized use promptly under their agreements.

11. Rights and requests

Subject to jurisdiction, you may request access, confirmation of processing, correction, deletion, a copy or portability, withdrawal of applicable consent, limits on sensitive uses, opt-out of sale/sharing or certain profiling, and appeals of denied requests. These rights extend where applicable to residents without accounts. Contact hello@caredaily.ai; we may verify identity or legal representative authority proportionately. An organizational controller may be responsible for some requests, and we may route the request to it and assist as required. Exercising privacy rights does not require downloading our app. We will not unlawfully discriminate for exercising applicable rights.

12. Washington consumer health data notice

For persons covered by Washington's My Health My Data Act, we may collect consumer health data comprising device-linked activity, rest, occupancy, mobility, fall-related events, wellness inferences, and care needs, from residents/representatives, devices, authorized organizations, and support interactions. We use it to provide requested ambient wellness and care-support services, deliver agreed insights/alerts, manage access, and maintain security. We share only as permitted with applicable service providers, sponsoring organizations, authorized Trusted Circle members, optional monitoring providers or legally required recipients. We currently do not identify independent corporate affiliates receiving consumer health data for separate purposes in the ordinary course, and Care Daily does not sell consumer health data.

Except where the statutory requested-service exception or another lawful ground applies, collection requires the consumer's prior consent for the specified purpose, and sharing requires a **separate** prior consent. Consent requests will identify categories of data, purposes, classes of recipients and withdrawal routes. An organization's request to purchase a Home subscription is not necessarily a request by the individual to whom the data relates. Additional categories or purposes require updated disclosures and affirmative consent where law requires. To exercise applicable rights or appeal a decision, write hello@caredaily.ai with subject "Consumer Health Data" or "Privacy Appeal." We provide required information about further appeals or agency complaints in any denial notice.

13. International and special-category data

Where services operate outside the United States, data may be processed in the US or other authorized processing locations. Additional data transfer safeguards, local notices, processor agreements, special-category lawful grounds and consent rules may apply. Telecoms and white-label partners launching in other countries must agree on controller/processor roles and localized notices before deployment; a US consumer form alone is not an adequate

substitute for local requirements. EU/UK health-related special-category data is handled under applicable legal grounds and additional Article 9 conditions where applicable.

14. Children, changes, and contact

We do not direct independent accounts to children under 13. A parent or lawful guardian may use a covered Home service to support a child, subject to specific applicable child privacy requirements. We may update this Policy by posting a new dated version and giving additional notice where legally required. A posted update is not itself consent to new collection, sharing, or uses when a law requires an affirmative choice. We will seek any additional consent or authorization that applies before the newly covered processing. Legal and privacy contact: People Power Company d/b/a Care Daily, Attn: Privacy; hello@caredaily.ai. Consumers, including residents without an app account, may exercise privacy rights through this address. For postal privacy correspondence, request our current business mailing address by email. The public website will maintain a prominent link to this Policy and, where applicable, the consumer-health-data notice.