Privacy Notice

How Reedstem, LLC handles personal information for HCBS MedPass

Reedstem, LLC · Aurora, Colorado, United States · hcbsmed.com
Last updated October 25, 2026 · Version 1.0

Contents

1. Who This Notice Covers
2. Information We Collect
3. How We Use Information
4. How We Disclose Information
5. Retention
6. Security
7. Where Information Is Processed
8. Children
9. Your Privacy Rights
10. State-Specific Information
11. Communications
12. Changes to This Notice
13. Contact Us

This Privacy Notice explains how **Reedstem, LLC** ("Reedstem," "we," "us"), the company behind **HCBS MedPass** ("MedPass" or the "Service"), collects, uses, discloses, and protects personal information. It also explains the choices and rights you have. Reedstem is located in Aurora, Colorado, United States, and its current contact details are published at hcbsmed.com.

1. Who This Notice Covers

This Notice applies to:

- **Visitors** to hcbsmed.com and the MedPass sign-in and contact pages.
- **Prospects** who request an account or contact us.
- **Account users**: the owners, administrators, nurses, direct care workers, and other staff whom our customers authorize to use MedPass ("Users"), for the account and usage information we handle about them.
- **Billing contacts** of customer organizations.

1.1 Residents' health information

Information about the residents, clients, and patients that our customers serve, including their health and medication records, is **Protected Health Information (PHI)**. We handle it only on behalf of our customers, as their business associate under HIPAA and under a Business Associate Agreement.

The customer (your care provider) controls that information. Its use and disclosure are governed by HIPAA and by the provider's own Notice of Privacy Practices, not by this Notice.

If you are a resident or a resident's representative and want to see, correct, or ask about your records, please contact your care provider. If you contact us, we will refer your request to the provider and help it respond.

1.2 Information about customers' staff

We also handle staff information that customers enter into MedPass, such as personnel files, credentials, and schedules, on the customer's behalf and under its instructions. Requests about that information should go to your employer.

2. Information We Collect

2.1 Information you give us

- **Contact and account-request details:** name, email address, phone number, job title, organization name, state, facility type, approximate number of locations and residents, and your message.
- **Account details:** name, email address, phone number, job title (discipline), credentials and license numbers, role and permissions, the branches you work in, and your password. Passwords are stored only as a one-way hash.
- **Billing details:** billing contact, billing address, tax identifiers if provided, plan, invoices, and payment status. Card and bank details are entered directly with our payment processor, Stripe. We receive only limited information such as card brand, last four digits, and expiration date. We never receive or store full card numbers.
- **Support communications:** messages you send through "Contact support," email, or phone, and our replies.

2.2 Information collected automatically

- **Security and audit logs:** sign-in times, IP address, actions taken in the Service (for example, records viewed or changed), and device or room-station identifiers. HIPAA requires these logs, and we use them to protect accounts and records.
- **Technical data:** browser or app type and version, operating system, and error reports needed to operate and fix the Service.
- **Local storage:** the MedPass app stores your session token, the server address, the device mode, and similar preferences on your device so that you stay signed in and the app works.

We do **not** use advertising cookies, cross-site tracking, or third-party analytics that profile you for advertising.

2.3 Information from others

- Your employer or organization when it creates your User account.
- Our payment processor, which provides payment status and limited card details.
- Our email provider, which provides delivery status.

3. How We Use Information

We use personal information to:

- provide, operate, maintain, and secure the Service, including authenticating Users and enforcing permissions;
- set up accounts and send login details, temporary passwords, and service notices such as renewal, payment, branch-deletion, and security notices;
- process subscriptions, invoices, payment reminders, and taxes;
- respond to requests and provide customer support;
- detect, investigate, and prevent security incidents, fraud, abuse, and violations of our Terms;
- monitor and improve performance and reliability, and develop new features, using de-identified or aggregate information where possible;
- comply with law, regulatory requests, and our obligations under Business Associate Agreements;
- establish, exercise, or defend legal claims.

We do not use PHI for marketing. We use and disclose PHI only as our Business Associate Agreements with customers permit.

4. How We Disclose Information

We disclose personal information only as follows:

- **To service providers (subprocessors)** that help us run the Service under contracts requiring them to protect it, and, for PHI, under business associate agreements where required:
- cloud hosting and database services (Google Cloud and Firebase, United States regions);
- payment processing (Stripe);
- email delivery (our business email provider).
- **To your organization:** owners and administrators of the customer account can see Users' account details and activity in audit logs.
- **For legal reasons:** to comply with law, subpoena, court order, or a lawful request from a government authority; to protect the rights, property, or safety of Reedstem, our customers, residents, or others; or to enforce our agreements.
- **In a business transfer:** to a buyer or successor in a merger, acquisition, financing, or sale of assets. The successor remains bound by this Notice and by applicable Business Associate Agreements.
- **With your direction or consent.**

We do not sell personal information, and we do not share it for cross-context behavioral advertising or targeted advertising. We have not done so in the past twelve months.

5. Retention

We keep personal information only as long as needed for the purposes described in this Notice:

- **Account and usage information** is kept for the life of the customer's subscription. When a customer account is closed, it is deleted with the customer's data after the 60-day export period described in our Terms of Service, or sooner on the customer's written request.
- **Encrypted backups** are overwritten in the ordinary course, generally within about thirty (30) days.
- **Billing and tax records** are kept as long as accounting and tax laws require, generally seven (7) years.
- **Contact and account requests** that do not become customers are kept for up to two (2) years, unless you ask us to delete them sooner.
- **Security logs** are kept as long as the customer account exists, or longer if needed to investigate an incident or as required by law.

6. Security

We protect information with administrative, physical, and technical safeguards designed to meet the HIPAA Security Rule. These include:

- encryption in transit (TLS) and at rest;
- additional field-level encryption for especially sensitive identifiers;
- role-based access controls;
- audit logging;
- secure software development practices;
- least-privilege access for our personnel;
- automated backups with point-in-time recovery.

No method of transmission or storage is completely secure. If we learn of a security incident affecting your information, we will notify the affected customer, and you where required, as required by HIPAA, state

breach-notification laws, and our agreements.

7. Where Information Is Processed

We process and store information in the United States. The Service is intended for use by organizations operating in the United States.

8. Children

The Service is not directed to children, and we do not knowingly collect personal information from children under 13 (or under 16 where state law sets that age) outside the PHI our customers enter about the people they serve. If you believe a child has given us personal information directly, contact us and we will delete it.

9. Your Privacy Rights

Depending on where you live, you may have rights over your personal information. Several U.S. states have comprehensive privacy laws, including California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Iowa, Indiana, Tennessee, Delaware, New Hampshire, New Jersey, Nebraska, Kentucky, Maryland, Minnesota, and Rhode Island. Subject to the exceptions in those laws, your rights may include the right to:

- know or access the personal information we hold about you;
- correct inaccurate personal information;
- delete personal information;
- obtain a portable copy;
- opt out of the sale of personal information, targeted advertising, and certain profiling (we do not do these things);
- limit the use of sensitive personal information (we use it only as needed to provide the Service);
- not be discriminated against for exercising your rights.

9.1 Information these rights do not cover

Many of these laws do not apply to PHI governed by HIPAA, or to information processed for a business customer as a service provider. For example, requests about records that your employer or care provider keeps in MedPass should go to that organization. We will help it respond.

9.2 How to make a request

Email support@hcbsmed.com with the subject line "Privacy Request," and tell us which right you want to exercise and how to reach you.

We will verify your identity by matching information you provide to information we hold. For account Users, we may ask you to confirm from your registered email address.

You may use an authorized agent where the law allows. We may ask the agent for signed permission and may verify your identity directly.

We respond within the time the law requires, generally forty-five (45) days. We may extend that once where permitted, with notice.

9.3 Appeals

If we deny your request, you may appeal by replying to our decision with the subject line "Privacy Appeal." We will respond within the time the law requires. If you are not satisfied, you may contact your state Attorney General.

9.4 Global Privacy Control

We do not sell or share personal information or use it for targeted advertising, so there is nothing to opt out of. We nevertheless treat a Global Privacy Control signal as a valid opt-out request where the law requires.

10. State-Specific Information

10.1 California

Categories collected in the past 12 months:

- identifiers (name, email, phone, IP address);
- customer records (billing contact, limited payment details);
- professional or employment information (job title, credentials);
- internet or network activity (audit and security logs);
- sensitive personal information limited to account log-in credentials.

Sources are described in Section 2, our **purposes** in Section 3, and our **disclosures** in Section 4. We do not sell or share personal information.

Under California's "Shine the Light" law, we do not disclose personal information to third parties for their direct-marketing purposes. Medical information we handle for providers is protected under HIPAA and the California Confidentiality of Medical Information Act through our agreements with those providers.

10.2 Colorado

Reedstem is based in Colorado. Colorado residents may exercise the rights in Section 9 under the Colorado Privacy Act, to the extent it applies.

10.3 Nevada

We do not sell covered information as defined by Nevada law.

10.4 Washington and other consumer-health-data laws

We do not collect "consumer health data" outside of PHI governed by HIPAA, which these laws exempt.

10.5 Texas

Information we handle on behalf of covered entities is protected as required by the Texas Medical Records Privacy Act through our agreements with those entities.

11. Communications

We send service emails, such as login details, security notices, invoices, payment reminders, renewal and contract notices, and branch-deletion notices. These are part of the Service, and you cannot opt out of them while you have an account. We do not send marketing emails to account Users without consent. If we send other updates, every message will include a way to unsubscribe.

12. Changes to This Notice

We may update this Notice. We will post the new version at hcbsmed.com with a new "last updated" date, and will notify customers of material changes by email or in the Service before they take effect.

13. Contact Us

Reedstem, LLC · HCBS MedPass · Aurora, Colorado, United States (mailing address at hcbsmed.com) · support@hcbsmed.com (subject: "Privacy Request" or "Privacy Question")

This Notice is provided as a professionally drafted template. It should be reviewed by qualified privacy counsel before publication.