

Privacy Notice for Physicians

Last updated: September 21, 2026

1. About this notice

Cadence Health Analytics Inc. ("Cadence", "we", "us") provides tools for patient questionnaires, score histories and clinic monitoring workflows. This notice covers physicians, authorized clinic staff and people who contact us about clinic access. It explains personal information handling in the app, on our website and in communications with Cadence.

For patient information processed through Cadence, your clinic remains responsible for its clinical records and the care it provides. Cadence processes information to provide the service. This notice does not replace your clinic's privacy obligations, patient-facing notices or any agreement governing processing on the clinic's behalf. The separate [Privacy Notice for Patients](#) explains the patient experience.

This notice explains our practices; it does not replace any consent or other authority needed for a particular collection, use or disclosure. Only submit patient or colleague information that you are authorized to provide.

2. Information we collect

- **Professional and account details:** name, email, telephone number, practice name, specialty, medical licence information where supplied, optional date of birth and profile photo, account identifiers, role and account status, and contact details selected for sharing.
- **Clinic and access information:** physician-patient assignments, staff permissions, invitations, approvals, clinic setup details, preferences and records of administrative actions.
- **Clinic enquiries:** contact name, work email, clinic name and role submitted through the clinic-interest form, together with contact permission, request status and onboarding history. Do not include patient health information in that form.
- **Clinical information:** patient profiles, caregiver contacts where entered, questionnaire responses, calculated scores, diagnoses, treatments, monitoring plans and appointment details where that feature is used.
- **Support and technical information:** support messages, account and notification activity, IP address, browser or device information, request times and operational or security logs. Firebase Authentication handles credentials, verification and sign-in information.

3. How we use information

We use information to establish and verify accounts; manage clinic access and staff permissions; present patient questionnaires, scores and treatment histories; support monitoring and permitted record transfers; respond to requests; troubleshoot and maintain the service; manage security; and meet applicable legal obligations.

We use contact information for invitations, verification, password resets, clinic onboarding, service messages and enabled reminders. An email provider processes the recipient address and message content. Messages can include a recipient's name, account links, clinic-interest details or a reminder that questionnaires are due.

Clinic-interest contact permission is used to respond about your clinic's interest and availability. It is not permission to add you to an unrelated marketing list. Non-essential promotional messages are separate from necessary account messages; you can ask us to stop them, and we obtain consent where required.

4. Access and disclosure

- **Patients and clinic colleagues:** linked patients can see physician profile and contact information used by the service. Additional contact details can have sharing controls. Authorized staff can access the physician workspace they are approved to assist. Review profile and staff settings before sharing information.
- **Clinical recipients:** patient records can be available to the linked physician, approved staff and a receiving physician through a permitted transfer or handoff. Downloading or sharing a report creates a copy that the receiving person or organization controls.
- **Cadence personnel:** administrators and support personnel may access information to operate the service, administer accounts, investigate issues and assist users, according to their responsibilities and permissions.
- **Service providers and lawful disclosures:** Google Cloud and Firebase support infrastructure, sign-in and storage; email and other operational providers process information needed to provide their services. Information may also be disclosed where law requires or permits it, or with the authorization required for the particular disclosure.

Research and other secondary uses. Research, product development or external statistical sharing beyond operating and supporting Cadence requires an appropriate legal basis, safeguards and any required consent. The purpose and recipients must be explained before a proposed use proceeds. This notice does not itself authorize unrelated use of identifiable patient information. Removing names or aggregating records does not automatically make data anonymous.

5. Hosting, location and safeguards

Cadence uses Google Cloud services, including Firebase, for application infrastructure. Firebase Authentication processes sign-in information in the United States. Other hosting, storage and email services may process information in Canada, the United States or other locations used by the relevant provider. We do not represent that all personal information stays in Canada. Information processed outside Canada may be subject to that country's laws and lawful government-access requirements.

Google describes service-specific processing in [Privacy and Security in Firebase](#). Contact Cadence for information about providers and processing arrangements relevant to your clinic; do not infer a particular database, file or backup location from the website's location.

Safeguards include authenticated access, role and clinic-assignment checks, encrypted HTTPS connections, and records of selected administrative actions. Your clinic should assign staff access appropriately and protect its devices and downloaded reports. No storage or transmission method can guarantee complete security.

Profile photos: uploaded patient and physician profile photos are delivered through publicly accessible image links. Anyone with a link can open the image. Photos are optional; do not upload health documents, identity documents or images that should not be accessible in this way.

6. Browser storage and external services

The app and its sign-in service use browser storage for session information, workspace selection and preferences. Browser storage may also hold unsent work. Patient questionnaire drafts can contain answers and free text and can survive sign-out in the same tab. Older drafts are discarded when checked after 24 hours; this is not an exact-time browser erasure guarantee.

Sign out and close the Cadence tab on shared devices. Clear saved site data if the browser restores previous sessions. Disabling browser storage can prevent sign-in or remove unfinished work. Downloaded reports remain on the device until you remove them.

The custom Cadence portfolio website does not include advertising trackers or an analytics SDK. Its host can process ordinary request and security logs. Sites reached through external links have their own privacy notices. Emails sent through a personal or clinic mailbox also pass through the sender's and recipient's email providers.

7. Retention, account closure and transfers

Retention depends on the purpose of the information, clinic recordkeeping requirements, account administration, security and applicable law. Contact Cadence to discuss access termination, records transfer or deletion.

Closing a physician account may require a handoff so that patients and clinical history are not left without a responsible physician.

Deletion from active systems does not necessarily remove all information. Clinical provenance and administrative audit records can remain, including names, email addresses and account identifiers. Providers and backups may retain copies. Copies already downloaded or held by your clinic are outside the app's account-deletion process. Contact us for the arrangements applicable to your request; there is no promise of immediate erasure of every copy.

8. Access, corrections and consent choices

Review and update supported profile fields in the app, or contact Cadence to request access to or correction of your account, enquiry or support information. We may verify your identity and authority. Patient requests concerning a clinic's medical record should be handled by the clinic, with Cadence assisting for information it processes on the clinic's behalf.

You can ask to withdraw consent for a use that relies on your consent, subject to applicable legal or contractual limits. We will explain the effect on the service. Withdrawal does not undo earlier lawful processing or override clinical recordkeeping requirements. You can decline optional information and non-essential communications; necessary account and security messages may still be sent.

9. Contact and complaints

Contact **Cadence Health Analytics Inc., Privacy enquiries**, at cadence.health.analytics@gmail.com or [+1 226 787 9704](tel:+12267879704). Postal address: 1206 Chilver Road, Windsor, Ontario, Canada, N8Y 2L1. Begin with your request and contact details rather than emailing patient records; we can discuss how to provide any sensitive information needed to resolve it.

You may contact the [Information and Privacy Commissioner of Ontario](#) about Ontario health privacy, or the [Office of the Privacy Commissioner of Canada](#) for matters within its jurisdiction. This notice is governed by Ontario law and the applicable laws of Canada. It does not limit rights or obligations under applicable law.

10. Changes to this notice

We will post revisions with an updated date and communicate material changes through the service or other appropriate means. If a new purpose requires consent, an updated notice alone does not supply it.