

privacy

Privacy Policy

ChronicGPT Inc. (“ChronicGPT,” “we,” “us,” or “our”) operates the ChronicGPT mobile application, website at <https://chronicgpt.com>, and related services (collectively, the “Services”). This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information when you use the Services.

This Policy is available in English, Hindi, and Tamil. All language versions are intended to be equivalent. If a discrepancy exists among language versions, the English version controls to the extent permitted by applicable law.

Privacy at a glance

ChronicGPT is a health and wellness application for adults in the United States, Singapore, and India. We collect information needed to operate your account, personalize coaching, and support the features you choose to use—including health information you enter, Symptom Checker assessments, and Apple Health data you authorize. We do not sell personal information or health information, and we do not use health information for advertising.

You may delete your account in the app under **Settings tab** → **Account Delete**. Sign-in ends immediately; removal of stored data on our servers is permanent and typically completes within 72 hours, subject to limited legal, security, and audit exceptions described below. We do not offer a self-serve downloadable data-export package in the app. Where required by law, you may request access to or a summary of your personal data by email. For privacy-policy questions, contact **privacy@chronicgpt.com**. For privacy rights, grievances, and Data Protection Officer matters, contact **grievance@chronicgpt.com** as described in Sections 14, 15, and 18.

1. Who we are and scope

ChronicGPT Inc., doing business as ChronicGPT, provides digital health and wellness coaching through structured programs, meal and activity logging, optional Apple Health integration, Symptom Checker educational assessments, and AI-assisted coaching features.

The Services are intended for users who are at least 18 years old and located in the **United States, Singapore, or India**. They are not directed to children, teenagers, or users outside those jurisdictions unless we separately launch in another jurisdiction and update this Policy.

Servers that host and process Service data are located primarily in the United States. If you use the Services from Singapore or India, your information is transferred to and processed in the United States as described in this Policy.

2. Information we collect

We collect only the information reasonably necessary to provide, secure, and improve the Services. Depending on the features you use, we may collect:

Account and contact information. Name, email address, optional phone number, password credentials, authentication identifiers, preferred language, and account settings.

Profile and demographic information. Age or date of birth, sex assigned at birth, gender, height, weight, state or country, and other profile details you choose to provide.

Health and wellness information. Health conditions, medications, allergies, goals, food and nutrition logs, glucose values, heart rate, sleep, activity, weight, health observations you add in the app, and related information you enter or authorize us to receive.

Symptom Checker information. Symptom descriptions and health complaints you enter in plain language; clarification and follow-up answers; structured summaries you review; safety acknowledgements; AI-generated educational assessment output; and persisted Symptom Checker history that you may view or delete in the app.

Fitness and activity information. Workouts and activity you log, and fitness-related data imported from Apple Health when you authorize access.

Photos and images. Images you choose to upload or capture for meal logging, barcode scanning, profile photos, and AI Doctor avatars.

AI and coaching information. Messages, chat content, generated responses, safety signals, and related coaching interactions.

Device and service-operation information. App version and limited security or operational logs needed to authenticate you, prevent abuse, troubleshoot errors, and maintain the Services. Our infrastructure may process IP addresses in access and security logs; we do not use those logs for advertising, marketing, or cross-app tracking, and we do not collect advertising identifiers.

We treat health, medication, Apple Health, Symptom Checker, and related wellness information as sensitive even when a specific law does not label it that way.

3. How we collect information

Directly from you. When you create an account, complete your profile, enroll in a program, log meals or activity, use AI Doctor coaching, use the Symptom Checker, configure Auto Log rules, manage medications, upload photos, or contact us.

From Apple Health, with your permission. When you choose to connect Apple Health, we read only the HealthKit categories needed for the feature you use. See Section 5.

From service providers. Such as cloud hosting, authentication, and AI processing providers that support the Services on our behalf.

Automatically. Through limited security and access logs needed to maintain reliability and security. We do not use a third-party crash or advertising analytics SDK in the current iOS app.

You may choose not to provide some information, but certain features may not work without it. For example, glucose coaching requires glucose data; meal guidance requires meal or nutrition information; Symptom Checker assessments require the symptom details and answers you provide.

4. Programs and feature-specific collection

ChronicGPT offers free 12-week cohort programs, including the **Weight-loss cohort** and the **Glucose-wellness cohort**. Program enrollment does not require payment.

If you enroll in the **Glucose-wellness cohort**, we may request permission to read blood glucose from Apple Health and process glucose-related information you log for coaching, trends, and program features. If you enroll only in the **Weight-loss cohort**, blood glucose is not requested from Apple Health unless you later enroll in the Glucose-wellness cohort.

Medication tracking, related features, and the **Symptom Checker** are available only to users whose date of birth on file confirms they are 18 or older.

Symptom Checker

When you use the Symptom Checker, we process your complaint text, follow-up answers, medical and profile context already on file (such as conditions and medications), AI-generated educational assessment content, safety-stop signals, and related history records. Assessment content may be generated using AI service providers under contractual and technical controls. Symptom Checker output is for education only and is not a diagnosis, treatment plan, or emergency service. You may delete individual Symptom Checker records from history in the app, and account deletion removes remaining Symptom Checker data with your other stored data.

We do not offer in-app purchases, telehealth visits, clinician review, separate CGM or wearable account linking, or a self-serve downloadable data-export package. Access and copy requests may be made through the rights channels in Sections 14, 15, and 18 where required by law.

5. Apple Health, camera, and other permissions

Apple Health / HealthKit

Device health data is imported through **Apple Health / HealthKit only**. We do not offer separate CGM pairing or third-party wearable account connections in the mobile app.

Apple Health connection is **optional**. During program enrollment step 2 you may tap **Not now** to skip connection and continue setup, or tap **Connect** after the in-app pre-consent screen to open the system HealthKit permission sheet. You may also connect later from **Me → Apple Health**.

When you authorize access, we may read these HealthKit categories:

- Workouts
- Heart rate
- Heart rate variability (HRV)
- Sleep analysis
- Blood glucose (**Glucose-wellness cohort** only)

What we do not read: step count, activity rings, workout GPS routes, clinical records, or ECG.

If you tap **Connect** at enrollment step 2, we request the system HealthKit permission sheet after the in-app pre-consent screen and import recent data to your account—including a **3-day bootstrap import** when you connect at that step. At enrollment step 3 (Data Import), you may tap **Continue anyway** if Apple Health is not connected. After enrollment, **Me → Apple Health** supports manual re-import up to **90 days per import** and a **Connect with my Apple Health** toggle for background sync (enrolled users only).

When cloud sync is enabled, newer readings may sync incrementally while you use relevant health features. Background updates use Apple's HealthKit background delivery entitlement, not remote push notifications or generic background modes.

After enrollment, the Activity, Sleep, Heart Metrics, and Glucose tabs show feature-scoped banner copy before the system permission sheet when you tap Allow access—not separate modal pre-consent sheets.

You control Apple Health permissions in the Health app and iOS Settings. If you revoke access, future syncing stops. Data already imported may remain until you delete your account, subject to the retention rules below.

We use Apple Health data only to provide health, wellness, coaching, and user-facing analytics features. We do not use Apple Health data for advertising, targeted advertising, marketing attribution, data-broker disclosure, unrelated product development, or training public foundation models. The app does not write data to Apple Health.

Camera, photos, and notifications

- **Camera** may be used to scan barcodes and capture meal images.
- **Photo library** may be used for meal photos, profile images, and images you choose to upload.
- **Local notifications** may be used for reminders you enable in the app.

The app does not request microphone access or device GPS location.

6. How we use information

We use information to:

- Create and secure your account; authenticate you; provide support; and maintain the Services.
- Operate program enrollment, goals, nutrition and activity tracking, medication logging, sleep and heart metrics coaching, Symptom Checker educational assessments, and AI Doctor coaching.
- Import, display, and analyze Apple Health data you authorize.
- Generate personalized insights, summaries, trend analysis, coaching responses, and Symptom Checker educational output.
- Operate AI features, detect potential safety concerns, and provide non-emergency safety guidance.
- Send local reminders and in-app messages you enable.
- Maintain reliability, prevent fraud and misuse, troubleshoot errors, and protect users and our systems.
- Improve the Services using aggregated, de-identified, or pseudonymized information where practical.
- Comply with applicable law, enforce our terms, and respond to valid legal process.

We do not train public foundation models on your identifiable health information. Where we use service providers for AI or cloud processing, we design requests to exclude account identifiers—such as your name, email, phone number, and internal user ID—where practical. Some flows may redact common contact details in free text before sending content to AI providers, but coverage varies by feature. We use contractual and technical controls designed to restrict service providers from using your information for purposes other than providing services to us.

7. AI and health safety

ChronicGPT uses artificial intelligence and rules-based logic to provide health and wellness support, including the Symptom Checker. AI-generated content may be inaccurate, incomplete, biased, or unsuitable for your circumstances.

ChronicGPT is **not an emergency service** and does not replace a licensed clinician. Do not use the Services as the sole basis for diagnosis, medication changes, or urgent medical decisions. If you may be experiencing a medical emergency, call **911 (United States)**, **995 (Singapore)**, **112 (India)**, or your local emergency number, or seek immediate emergency care.

Human clinician review, telehealth visits, and prescription services are not offered through the mobile app.

8. How we disclose information

We do not sell your personal information or health information. We disclose information only as reasonably necessary to:

- **Service providers** that support hosting, cloud storage, authentication, security, customer support, and AI processing, subject to contractual obligations to protect information and use it only for authorized purposes.
- **People or organizations you direct us to share with**, when a sharing feature is available and you choose to use it.
- **Legal, safety, and compliance purposes**, including responding to valid legal process or protecting against serious harm, fraud, or security threats.
- **Business transactions**, such as a merger, financing, acquisition, reorganization, or sale of assets, subject to confidentiality protections.
- **Aggregated or de-identified information** that does not reasonably identify you, for analytics, product improvement, safety evaluation, or business reporting.

We do not share health, fitness, medication, Apple Health, Symptom Checker, or conversation data with advertising platforms, data brokers, or third-party ad networks.

9. Analytics, advertising, and tracking

We may use limited analytics and diagnostics to understand app performance, crashes, and aggregate feature use. We do not use health information, Apple Health information, health conditions, medications, diagnoses, Symptom Checker content, conversation content, or other sensitive health information for advertising, targeted advertising, marketing attribution, or disclosure to data brokers.

We do not track you across third-party apps or websites for advertising purposes.

10. Communications

The mobile app uses **local scheduled notifications** and in-app messages for reminders you enable. The app does not send remote push notifications, SMS, or WhatsApp messages.

After you confirm account deletion in the app (**Settings tab** → **Account Delete**), we may send a one-time confirmation email to your registered address acknowledging the request. That email is not a copy or export of your data and cannot be used to cancel deletion. If you did not request deletion, contact support@chronicgpt.com immediately.

If we introduce additional communication channels on other surfaces in the future, we will describe them in an updated policy and, where required, obtain appropriate consent.

11. Retention, deletion, and your choices

We retain personal information only for as long as reasonably necessary to provide the Services and meet legal, security, audit, dispute-resolution, and compliance obligations.

Account deletion

You may permanently delete your account in the app under **Settings tab** → **Account Delete**. Sign-in is removed immediately and you are signed out. We then delete your stored account data from our active systems; that process typically completes within **72 hours**, subject to limited retention described below. Deletion is permanent. In-app Account Delete is the primary deletion path. If you need assistance with deletion, or if a legal right requires us to act on a written request, contact **grievance@chronicgpt.com**. We do not offer a self-serve downloadable data-export package. Where required by law, we will handle access or copy requests through the rights channels in Sections 14, 15, and 18. We may send a one-time confirmation email to your registered address acknowledging the deletion request, as described in Section 10.

AI Doctor deletion

You may delete your AI Doctor in the app under **AI Doctor tab** → **Picture** → **Delete** without deleting your entire account. This removes your AI Doctor profile, training data, and detected patterns from our servers while your account and other logs remain. That process may also take up to 72 hours. We do not send email confirmation for AI Doctor deletion.

Symptom Checker history

You may delete individual Symptom Checker records from history in the app. Remaining Symptom Checker data is removed with account deletion under **Settings tab** → **Account Delete**.

Program unenrollment

Unenrolling from a cohort program ends that program enrollment but does not delete your account or other stored data.

Other choices

You may update profile information in the app. You may revoke Apple Health permissions in iOS Settings at any time.

We may retain only the minimum information necessary to comply with law, resolve a dispute, protect security, prevent fraud, or maintain a deletion-compliance record. Encrypted backup copies may persist for a limited period until overwritten under our backup lifecycle.

Privacy questions and rights requests

For privacy-policy and data-practices questions, email privacy@chronicgpt.com. For access, correction, consent withdrawal, grievance, nomination, or other privacy-rights requests, email grievance@chronicgpt.com (see Sections 14, 15, and 18). We will verify your identity before releasing personal data and respond within the timelines described in those sections.

12. Security

We use administrative, technical, and physical safeguards designed to protect personal and health information, including encryption in transit and at rest, least-privilege access controls, authentication protections, access logging, security monitoring, and vendor controls. No system is completely secure, and we cannot guarantee absolute security.

13. U.S. privacy rights

Depending on your state and the information involved, you may have rights regarding access to, correction of, deletion of, or information about our processing of your personal information.

For the mobile app, account deletion under **Settings tab** → **Account Delete** is the primary way to remove your account and stored data. You may update certain profile information in the app. Where a legal obligation requires access, correction, or similar support that cannot be completed through in-app controls alone, email grievance@chronicgpt.com or privacy@chronicgpt.com, or write to us as described in Section 18. We do not offer a self-serve downloadable data-export package; where access or a summary is required by law, we will fulfill that request through the rights channel after identity verification.

14. Singapore personal data (PDPA)

If you are in Singapore, our processing of personal data is intended to comply with Singapore's Personal Data Protection Act 2012 (PDPA) where it applies.

Purposes, consent, and withdrawal

We collect and use your personal data for the purposes described in this Policy, including providing the Services, personalizing coaching, operating the Symptom Checker, securing accounts, and complying with law. Where required, we rely on your account signup, acknowledgements, and in-app permissions as consent for the stated purposes. You may withdraw consent for optional processing (for example, Apple Health access) in the app or by emailing grievance@chronicgpt.com. Withdrawal does not affect processing already completed. If consent is required for a feature and you withdraw it, that feature may become unavailable.

Access and correction

You may request access to, or correction of, your personal data by emailing **grievance@chronicgpt.com**. We aim to respond within about **30 days** of receiving a verified request, or to provide a written progress notice if more time is reasonably needed. You may also update certain profile fields in the app. We do not offer a self-serve downloadable export package; access and copy requests are fulfilled through this channel where required.

Overseas transfer

Your personal data is transferred to and stored on servers in the United States. We use contractual and technical measures designed to provide a standard of protection comparable to that under the PDPA for personal data transferred outside Singapore.

Complaints and DPO

If you have a privacy complaint or wish to contact our Data Protection Officer, email **grievance@chronicgpt.com**, call **+91 99449 02046**, or write to either address in Section 18. Our designated Data Protection Officer is **Arasi Balaji, MD**. You may also lodge a complaint with the Personal Data Protection Commission (PDPC) of Singapore where applicable.

Account deletion

You may permanently delete your account and stored data under **Settings tab** → **Account Delete**. For deletion assistance or related rights requests, contact **grievance@chronicgpt.com**.

Notifiable data breaches

If a data breach occurs that is notifiable under the PDPA, we will assess the incident promptly and notify the PDPC and affected individuals as required by law.

15. India personal data (DPDP Act and SPDI Rules)

If you are in India, our processing of personal data is intended to comply with India's Digital Personal Data Protection Act, 2023 (DPDP Act) and, where still relevant, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).

Purposes, consent, and withdrawal

We process your personal data to provide the Services you request, including account operation, wellness coaching, Symptom Checker assessments, Apple Health imports you authorize, security, and legal compliance. Health and Symptom Checker information may constitute personal data related to health (or sensitive personal data under the SPDI Rules) and is processed only as needed for the features you use. You may withdraw

consent in writing by emailing **grievance@chronicgpt.com** or by using in-app controls where available (for example, revoking Apple Health permissions or deleting your account). Withdrawal does not affect processing already completed lawfully.

Access, correction, erasure, and nomination

Subject to applicable law, you may request:

- a summary of the personal data we hold about you and the processing activities relating to that data;
- correction, completion, or updating of your personal data;
- erasure of personal data that is no longer necessary for the stated purpose, including by using **Settings tab** → **Account Delete** or by requesting assistance at **grievance@chronicgpt.com**; and
- nomination of another adult to exercise your rights in the event of your death or incapacity, by emailing **grievance@chronicgpt.com** with the nominee's identity and contact details.

We do not offer a self-serve downloadable export package; access and summary requests are fulfilled through the rights channel after identity verification.

Cross-border processing

Your personal data is transferred to and processed in the United States. We use contractual and technical measures designed to protect personal data transferred outside India. We will comply with any applicable Central Government directions regarding restricted territories if and when they apply.

Grievance Officer

Our Grievance Officer for India is:

Arasi Balaji, MD, Managing Director, ChronicGPT Inc.

Email: **grievance@chronicgpt.com**

Phone: **+91 99449 02046**

Postal (India): **272 Sarveswarar Koil St, Anna Nagar, Madurai 625 020, India**

We aim to respond to grievances within **one month** of receipt (consistent with SPDI Rule 5(9)). As DPDP Rules come fully into force, we will also observe any outer grievance timeline required by those Rules (including the ninety-day outer bound where applicable). You may escalate unresolved grievances to the Data Protection Board of India where available under applicable law.

Personal data breaches

If a personal data breach occurs, we will take reasonable steps to contain and investigate it and will intimate affected individuals and the Data Protection Board of India as required by applicable law.

Account deletion

You may permanently delete your account and stored data under **Settings tab** → **Account Delete**. For deletion assistance or other rights requests, contact grievance@chronicgpt.com.

16. Children's privacy

The Services are intended for adults 18 years of age or older. We do not knowingly collect personal information from anyone under 18. If we learn that a person under 18 has provided information, we will take reasonable steps to delete it unless retention is required for safety, legal, or compliance reasons.

17. Changes to this policy

We may update this Policy as our Services, legal obligations, or privacy practices change. We will post the updated Policy with a new effective date. For material changes, we will provide additional notice as required by law, such as in-app notice or email.

18. Contact us

ChronicGPT Inc. (corporate headquarters)

5159 Steinbeck Circle
Flower Mound, TX 75022
United States

India Grievance Officer postal address

Arasi Balaji, Managing Director, ChronicGPT Inc.
272 Sarveswarar Koil St
Anna Nagar, Madurai 625 020
India

Privacy-policy questions: privacy@chronicgpt.com

Privacy rights, grievances, and Data Protection Officer / Grievance Officer (Arasi Balaji, MD): grievance@chronicgpt.com · +91 99449 02046

Account deletion (primary path): in the app under **Settings tab** → **Account Delete**. For deletion assistance or legally required written rights requests, email grievance@chronicgpt.com.

For formal written notices required by law, use either postal address above, as applicable.