

MOSAIC HEALTH ANALYTICS INC. PRIVACY POLICY

Last Updated: **January 7, 2026**

Mosaic Health Analytics Inc. (“we,” “us,” or “our”) takes the privacy of personal information very seriously. This Privacy Policy describes our practices with respect to the collection, use, disclosure, and protection of personal information.

This Privacy Policy applies to personal information that we collect and process in the course of providing our services in Canada and the United States (our “**Services**”), including our web and mobile applications (the “**App**”) and website located at <https://www.app.mosaicanalytics.health> (the “**Website**”).

TABLE OF CONTENTS

- About our Services
- Collection and Use of Personal Information
 - Patient Information – Canada (Provincial Health Legislation)
 - Patient Information – United States (HIPAA)
- Disclosure of Personal Information
- Information Collected Automatically
- Security of Personal Information
- Retention of Personal Information
- Use of Artificial Intelligence
- Your Rights
- Updates to our Privacy Policy
- Contact Us

ABOUT OUR SERVICES

We provide software tools that allow health care professionals, such as psychologists, psychiatrists, and therapists (“**Practitioners**”), to automatically generate clinical notes from their sessions with patients (“**Patients**”).

We collect personal information in two main capacities:

1. *Practitioner Personal Information (Independent Organization / Controller Role:* We collect personal information relating to Practitioners (for example, account information, billing details, support communications, and usage data) to promote, provide and administer our Services, and otherwise manage our relationship with Practitioners and their organizations. We refer to this information as “**Practitioner Personal Information.**” We are accountable for and in control of Practitioner Personal Information under applicable privacy laws in Canada and the United States.
2. *Patient Personal Information and Personal Health Information (Service Provider / Business Associate Role:* In providing our Services to Practitioners and their organizations (such as clinics and hospitals), we may collect and process personal information and personal health information relating to Patients. We refer to this

information as “**Patient Information**”. We process Patient Information on behalf of those organizations as their service provider in accordance with their instructions and our agreements with them.

PATIENT INFORMATION – CANADA

In **Canada**, we act as a service provider to “health information custodians” under applicable provincial health privacy laws. For example, where Ontario’s *Personal Health Information Protection Act, 2004* (“PHIPA”) applies, the Practitioner or clinic is the health information custodian and remains accountable for and in control of Patient Information.

We collect, use, and disclose personal health information only as permitted or required by:

- the instructions of the relevant health information custodian;
- our agreements with that custodian; and
- applicable law, including applicable provincial health privacy laws.

We rely on the custodian to obtain any consents required from Patients and to provide any required notices regarding the use of our Services. Custodians are responsible for deciding what personal health information is entered into our Services, and for determining how long to retain Patient records. We provide tools that allow Practitioners and clinics to manage and delete Patient information.

PATIENT INFORMATION – UNITED STATES (HIPAA)

In the **United States**, we act as a “business associate” under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“HIPAA”), and the Practitioner or clinic is typically a “covered entity.” As a business associate, we only use and disclose protected health information (“PHI”) as permitted by HIPAA and our agreements (including any Business Associate Agreement (“BAA”)).

We use and disclose PHI only:

- to perform the Services for the covered entity as described in our BAA, Subscription Agreement and related agreements;
- for our own proper management and administration or to carry out our legal responsibilities, as permitted by HIPAA; and
- as otherwise required by law.

We do not sell PHI or use it for marketing to Patients.

We do not permit our cloud providers (such as Microsoft Azure, including Azure OpenAI) to use PHI or other client data processed through our Services to train their foundation models.

We do not determine the purposes for which Patient information is collected or used by Practitioners and their organizations. Practitioners and their organizations, and Covered Entities under HIPAA, remain responsible for obtaining any consents or authorizations required for the use of our Services with their Patients , and for configuring their own retention and deletion rules.

Subject to our agreements with covered entities and applicable law, we may use *de-identified data* (which no longer identifies an individual and cannot reasonably be used to re-identify them, alone or in combination with other information) to maintain, improve and develop our Services. We do not attempt to re-identify individuals from de-identified data.

COLLECTION AND USE OF PERSONAL INFORMATION

Practitioner Accounts: To access the Services, Practitioners are required to create an account with us. We collect Practitioner name, title, email address, password, and mobile phone number for the purposes of administering the account and managing our relationship.

Payment information: We may collect and use payment card information (including payment card number, security code, expiration date, cardholder name and billing address) for the purposes of processing payments for our Services.

Inquiries: If you contact us with an inquiry, you may be asked for information that identifies you, such as your name, address and a telephone number, along with additional information we need to help us promptly answer your inquiry. We may retain this information to assist you in the future and to improve our customer service and service offerings.

Communications: We may use Practitioner Personal Information to communicate with Practitioners in connection with our Services, including for promotional purposes. Practitioners may opt-out of promotional communications by using the “unsubscribe” instructions provided, or by contacting us as set out below.

Patient Sessions: Our Services capture interactions between Practitioners and Patients to generate clinical notes for Practitioners. We use any Patient Personal Information (which may include personal health information and PHI) that we collect and process in the performance of these Services for the sole purposes of providing these Services to Practitioners and their organizations. This may include the use of Patient Personal Information for the proper management and administration of Mosaic, to improve or further develop our Services, and to carry out our legal responsibilities as permitted by applicable law and our agreements. When we use Patient Information for improvement or development purposes, we take steps to ensure that the information has been de-identified.

DISCLOSURE OF PERSONAL INFORMATION

We do not sell personal information. However, we may share personal information with third parties as described below.

ss and Cross-Border Transfers: In connection with our Services, we may transfer (or otherwise make available) personal information to third parties who provide services on our behalf. For example, we may use service providers to host our Services, store data and provide back-ups (including cloud-based service providers), process payments or provide logging and email services.

Personal information is primarily maintained and processed for Canadian data, in self-managed Canadian data centres . For US data, the data will be stored in self-managed US data centres.

Certain processing activities (for example, the processing of anonymized transcripts through Azure OpenAI) may occur in other jurisdictions.

Our service providers are given the information they need to perform their designated functions, and we do not authorize them to use or disclose personal information for their own purposes. We require our service providers to protect personal information in a manner consistent with this Privacy Policy and applicable law. We may update our list of key service providers from time to time; the current list of material subprocessors is available at <https://www.mosaicanalytics.health/documents/GraceNotes%20Subprocessor%20List.pdf> and we will provide notice of material changes where required by our agreements with clients.

Sale of Business: We may transfer personal information in connection with a prospective or completed amalgamation, merger, acquisition or sale (including transfers made as part of insolvency or bankruptcy proceedings) involving all or part of our business or assets or as part of a corporate reorganization or other change in corporate control.

Legal: We and our Canadian, US and other service providers may disclose your personal information in response to a search warrant or other legally valid inquiry or order (which may include lawful access by Canadian, US or other foreign governmental authorities, courts or law

enforcement agencies), to other organizations in the case of investigating a breach of an agreement or contravention of law or detecting, suppressing or preventing fraud, or as otherwise required or permitted by applicable Canadian, US or other law.

INFORMATION COLLECTED AUTOMATICALLY

Visiting our Website: We collect the IP (Internet protocol) addresses of all visitors to our Website and other related information such as page requests, browser type, operating system and average time spent on our Website. We use this information to help us understand our Website activity and to improve our Website.

Using our App: When you use our App, we collect information regarding your device type, operating system and version, carrier provider, unique device identifier, language setting, and the date and time that the App accesses our servers. We use this information to help us understand the activity on our App and to monitor and improve our App.

Cookies: Our Website uses a technology called “cookies”. A cookie is a tiny element of data that our Website sends to a user’s browser, which may then be stored on the user’s hard drive so that we can recognize the user when they return. We use cookies to remember your preferences and to authenticate you. You may set your browser to notify you when you receive a cookie or to not accept certain cookies. However, if you decide not to accept cookies from our Website, you may not be able to take advantage of all of the Website features.

Analytics and Marketing Technologies: We use third-party analytics and marketing tools, including services such as RB2B, to help us understand how visitors interact with our Website, measure the effectiveness of our marketing efforts, and identify organizations that may be interested in our services.

These technologies may collect information such as IP address, device and browser information, pages visited, and inferred professional or organizational information, which may be matched against third-party business or professional data sources (including LinkedIn-derived datasets). Where required by law, we obtain your consent before using these technologies. You may manage your cookie preferences at any time through our cookie banner or by adjusting your browser settings.

THIRD PARTY SITES

Our Website or App may contain links to other websites that we do not own or operate. We provide links to third party websites as a convenience to the user. We do not have any control over such websites, and therefore we have no responsibility or liability for the way the organizations that operate such linked websites may collect, use or disclose, secure and otherwise treat personal information. We encourage you to read the privacy policy of every website you visit.

SECURITY OF PERSONAL INFORMATION

We have implemented reasonable administrative, technical and physical safeguards in an effort to protect against unauthorized access, use, modification and disclosure of personal information in our custody and control, including policies and procedures governing our handling of personal information throughout its lifecycle. This includes safeguards designed to meet the requirements

of HIPAA for the PHI we process as a business associate and the safeguards required under provincial health privacy laws and other applicable Canadian laws and the laws of the United States for personal health information we process as a service provider. Both US and Canadian data centres employ Azure de-identification per-region, and anonymized text or ephemeral data is processed globally. Data collected in each region are architecturally separate from one another.

However, no security measures can offer absolute security and we cannot guarantee that your personal information will not be stolen or accessed without authorization.

RETENTION OF PERSONAL INFORMATION

Personal information is maintained on our servers or those of our service providers and is accessible by authorized employees, representatives and agents who require access for the purposes identified in this Privacy Policy.

We retain personal information for as long as necessary to fulfill the purposes described in this Privacy Policy or as otherwise required or permitted by law. In particular:

- *Audio streams.* Audio is processed only to generate transcripts and is deleted promptly after transcription is complete.
- *Transcripts.* By default, transcripts, which are intermediate processing of a patient session, are retained in our systems for up to thirty (30) days from creation, prior to conversion into Notes.
- *Notes.* Notes are retained indefinitely, until they are deleted by the Client.
- *User obligations.* Clients are responsible for configuring and applying their own retention rules and for deleting transcripts and notes in accordance with their legal and professional obligations.
- *Logs and audit trails.* System logs and audit trails are generally retained for up to seven (7) years for security, audit, and compliance purposes, unless a different period is agreed with a client or required by law.

Regardless of data type, data is stored in the region of origin and are architecturally separate. Upon termination of a Practitioner Account subscription, we will retain client data for a limited data export period (typically up to 90 days) to enable the client to export its data in then-available formats (for example, CSV or PDF), after which we will delete or de-identify the data from active systems, subject to any legal retention requirements.

USE OF ARTIFICIAL INTELLIGENCE

As part of our commitment to providing the Services, we may use artificial intelligence (AI) tools to assist in processing and analyzing personal information. These tools operate strictly within the scope of this Privacy Policy.

In particular:

- AI models are used to assist in generating draft clinical notes and related documentation from audio or text input.
- Human review is required. Our tools are intended to support, not replace, professional judgment. Practitioners are responsible for reviewing, correcting, and approving all drafts before relying on them for clinical or administrative purposes.
- We do not allow our third-party AI providers to use PHI or other client data processed through our Services to train their foundation models.
- AI outputs may contain errors or omissions and should not be treated as complete or authoritative records without human review.
- For Canadian and US deployments, PHI is stored and processed in-region (Canada or US) in Mosaic’s own environment.
- Anonymized or de-identified text may be processed by Azure OpenAI globally, but:
 - Microsoft does not store intermediate data or use it for training.
 - Mosaic ensures no PHI is used to train third-party foundation models.

YOUR RIGHTS

If you are a Patient, please contact your Practitioner to exercise any of your rights with respect to your Patient Personal Information.

If you are a Practitioner, you may request access to or correction of your personal information (subject to limited exceptions prescribed by law) by submitting a written request to our Privacy Officer (see “Contact Us” below). You may also have the right, in specified circumstances, to withdraw your consent to our processing of your personal information, or to request a copy of the information you have provided to us to use for your own purposes. If you have any questions about these rights, or you would like to exercise any of them, please contact us as described below. We will handle your request in accordance with our policies and may request certain personal information for the purposes of verifying your identity.

UPDATES TO OUR PRIVACY POLICY

This Privacy Policy may be updated periodically to reflect changes to our personal information practices. The revised Privacy Policy will be posted on our Website. We encourage you to refer to this Privacy Policy often for the latest information about our personal information practices.

CONTACT US

Please contact our Privacy Officer at **privacy@mosaicanalytics.health** if you have any questions, comments or complaints about this Privacy Policy or our practices with respect to the handling of Practitioner Personal Information or our role as a service provider/business associate.

If you are a Patient, please contact your Practitioner for any questions with respect to the handling of your Patient Information or PHI.