

Privacy Policy

For the purposes of Ontario's *Personal Health Information Protection Act*, 2004, Med Melanin Inc. acts as an agent to Health Information Custodians in relation to any Personal Health Information we handle.

This Privacy Policy, together with all schedules, appendices, attachments, any terms of service, and annexes (the "**Agreement**") (all of such documents are accessible via <https://www.medmelanin.com/>) and between Med Melanin Inc. and all its affiliates (together "**us**", "**we**", and/or "**our**") and you, the individual or company ("**you**", "**your**", and/or "**User**") governs your use of our website application, accessible at <https://www.medmelanin.com/>, and all pages, templates, products, tools, information, protocols, software, and content located therein (the "**Service**"), and explains how we collect, safeguard, and disclose information that results from your use of the Service. PLEASE READ THIS POLICY CAREFULLY.

1. Definitions

"**Cookies**" are small files stored on your device (computer or mobile device).

"**Data Controller**" means a natural or legal person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. For the purpose of this Privacy Policy, we are a Data Controller of your data.

"**Data Processors**" or "**Service Providers**" means any natural or legal person who processes the data on behalf of the Data Controller. We may use the services of various Service Providers in order to process your data more effectively.

"**Data Subject**" is any living individual who is the subject of Personal Data.

"**Device Information**" is information about the computer or mobile device that a user uses to access the Service, such as the hardware model, operating system and version, identification numbers assigned to the device, such as the ID for Advertising (IDFA) on Apple devices, and the Advertising ID on Android devices, mobile network information, and website or app usage behavior.

Healthcare Practitioners means practitioners who provide or assist in the provision of healthcare through our service, which may include nurse practitioners, nurses, physicians, mental health therapists, dietitians, and naturopaths

"**Location Information**" is information about the location of a user when the user accesses or

uses the Service. For example, via browser information and other similar device or browser attributes (like IP address), a locator page that may exist, or from a mobile application.

“Navigational Information” when a user accesses the Service, the user’s computer, phone, and/or device may provide navigational information, such as browser type and version, service-provider identification, IP address, the site or online service from which you came, and the site or online service to which you navigate.

“Personal Data” means data about an individual defined under s.3 of this Privacy Policy

“Personal Health Information” (“PHI”) – information about an identifiable individual that relates to physical or mental health, health services, payments, or provincial health-number identifiers.

“PHIPA” – the *Personal Health Information Protection Act, 2004* (Ontario), together with all current amendments and its companion regulation *O. Reg. 329/04*.

“Usage Data” is data collected automatically either generated by the use of Service or from Service infrastructure itself (for example, the duration of a page visit) by you.

2. Information Collection and Use

We collect several different types of information for various purposes to provide and improve our service to you, see § 3 below for more information on the types of information we collect from you. Additionally affiliated entities, vendors, social media networks, and advertising networks may provide us with, or supplement, information about you. We may use this information for a variety of operational or marketing purposes related to Personal Data only (non-PHI); we do not use PHI for advertising.

3. Types of Information Collected

Collection of Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you (**“Personal Data”**). Personal Data may include, but is not limited to:

(a) Name, address, phone number, email address, personal preferences, payment card number, purchase and ordering information, demographic information, responses to survey questions, your Location Information, your Navigational Information, your Device Information, your Usage Data, and any other information you choose to provide.

(b) We may use your Personal Data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt

out of receiving any, or all, of these communications from us by emailing at admin@medmelanin.com.

Collection of PHI

We collect PHI only as needed to deliver the service and comply with Ontario's PHIPA. PHI may include:

Identity details – name, date of birth, gender, provincial health-card number.

Contact details – mailing address, email, phone number.

Clinical records – diagnoses, treatment history, prescriptions, referrals, test and lab results uploaded or entered into the platform

Biometric and vitals data – height, weight, heart rate, blood pressure, glucose readings, or other device-generated measurements.

Wellness and lifestyle inputs – exercise logs, nutrition data, sleep patterns, stress levels, self-reported symptoms, survey answers, and goal-tracking information.

Care-related usage data – timestamps, feature interactions, and audit trails that show when and how you (or your care team) access PHI within the service.

All PHI is stored and processed in accordance with PHIPA, segregated from non-health personal data, and used only for the purposes described in the “Use of Data” section.

Usage Data

We may also collect information that your browser sends whenever you visit our Service or when you access Service by or through a mobile device (“**Usage Data**”).

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access Service with a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

Tracking Cookies Data

We may use cookies and similar tracking technologies to track the activity on our Service and we hold certain information.

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Other tracking technologies are also used such as beacons, tags and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we may use:

- (a) Session Cookies: We use Session Cookies to operate our Service.
- (b) Preference Cookies: We use Preference Cookies to remember your preferences and various settings.
- (c) Security Cookies: We use Security Cookies for security purposes.

4. Individual Rights Under PHIPA

Your rights to access, correct, or withdraw consent for PHI are described in Section 5 (Consent to collecting Personal Data and PHI).

5. Use of Personal Data and PHI

Personal Data

We use the collected Personal for various purposes:

- (a) to provide and maintain our Service;
- (b) to notify you about changes to our Service;
- (c) to allow you to participate in interactive features of our Service when you choose to do so;
- (d) to provide customer support;
- (e) to gather analysis or valuable information so that we can improve our Service;
- (f) to monitor the usage of our Service;
- (g) to detect, prevent and address technical issues;

- (h) to fulfill any other purpose for which you provide it;
- (i) to carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection;
- (j) to provide you with notices about your account and/or subscription, including expiration and renewal notices, email-instructions, etc.;
- (k) to provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information;
- (l) in any other way we may describe when you provide the information;
- (m) to aggregate pseudonymized or anonymized information for statistical or other purposes and,
- (n) for any other purpose with your consent.

Despite anything in this Section 5, Google Workspace APIs are not used to develop, improve, or train generalized AI and/or ML models.

Use of PHI

We use your PHI only for the following limited purposes:

- (a) Service delivery – to create and manage your account, enable the platform’s healthcare and wellness features, and support any clinicians or care teams that you authorize to access your PHI.
- (b) De-identified analytics – to measure performance, improve existing features, develop new tools, and generate statistical reports, but only after the data has been irreversibly de-identified so that no individual can be identified.
- (c) Legal and compliance obligations – to meet requirements under applicable laws, respond to lawful requests from regulators or courts, detect or prevent fraud or security threats, and keep necessary business records.
- (d) We do not sell PHI. We do not use PHI for marketing, fundraising, or advertising unless you provide a separate, explicit opt-in consent for that specific purpose.

6. Consent to collecting Personal Data and PHI

Collection of Personal Data

How do we get your consent?

When you provide Personal Data to use our software application, you give knowledgeable consent for us to collect and use that data solely to deliver the Service described on our website. If we ask for your Personal Data for a secondary reason, such as for marketing, we will either ask you directly for your express consent.

How do you withdraw your consent?

If you change your mind regarding your consent to our collection of your Personal Data, then you may withdraw your consent for us to contact you, for the continued collection, use or disclosure of your Personal Data, at any time by emailing us at admin@medmelanin.com.

Collection of PHI

Express and informed consent to collecting PHI

We will collect, use, or disclose your PHI only when you give clear, informed consent, unless the HIPAA permits or requires us to act without consent (for example, to prevent serious harm or comply with a court order).

Full explanation of purpose

Before or at the time we seek your consent, we will explain in plain language what PHI we need, why we need it, how we will use it, to whom we may disclose it, and any significant risks or benefits a reasonable person would want to know.

How you give consent

You provide consent by taking a positive action, such as clicking “Accept,” signing electronically, or verbally confirming in a recorded call. Consent is never assumed or implied.

Right to withdraw consent

You may withdraw consent at any time by emailing admin@medmelanin.com or by using the in-app privacy settings. Withdrawal will not affect PHI already processed, but it may limit our ability to continue providing certain services.

Substitute decision makers and Minors

If you are incapable of consenting, or the PHI relates to a Minor (i.e. under the age of 18 years old), an authorized substitute decision maker may grant, refuse, or withdraw consent on your behalf in accordance with PHIPA.

No marketing without separate opt-in

We will not use PHI for marketing, fundraising, or advertising unless you give a separate and explicit opt-in consent for that specific purpose.

Record of consent

We keep an auditable record of every consent and withdrawal, including the date, method, PHI involved, and the purposes you authorized.

Contact for questions or requests

To ask questions, withdraw consent, or exercise any privacy rights, contact our Privacy Officer at admin@medmelanin.com.

7. Retention of Personal Data and PHI

Retention of personal health information

We keep your personal health information (“PHI”) only for as long as is reasonably necessary to deliver the service you have requested and to meet any ongoing legal or regulatory obligations under the PHIPA. Once those purposes have been fulfilled, we securely destroy the PHI or irreversibly de-identify it as soon as practicable, and in any event within a commercially reasonable period, using industry-standard media-sanitisation methods.

Retention of Personal Data

We retain your Personal Data only for as long as necessary for the purposes described in this Privacy Policy. We keep and use this data to comply with legal obligations, resolve disputes, and enforce our agreements and policies. Usage data held solely for internal analysis is generally kept for a shorter period, unless it is needed to strengthen security, improve the service, or satisfy a legal requirement.

8. Transfer of Data

Cross-border transfer of Personal Data

We may use cloud infrastructure or service providers in other jurisdictions to deliver and support the platform. When this occurs, only Personal Data, not PHI, is transferred. Before any such transfer, we ensure the recipient offers privacy and security protections that are contractually equivalent to Ontario standards, including encryption, access controls, and breach-notification duties.

Storage and processing of PHI in Canada

We store and process your PHI exclusively on servers located in Canada. We will not transmit, disclose, or back-up PHI outside Canada unless you give us express consent for the transfer. Any permitted transfer occurs only under a written agreement that:

- limits the recipient to the authorised purpose;
- requires safeguards that provide a level of protection substantially similar to Ontario's PHIPA, including encryption in transit and at rest, strict access controls, breach-notification duties, and audit rights; and
- obliges the recipient to delete or return the PHI once it is no longer required.

9. Disclosure of Personal Data and PHI

Disclosures that may involve PHI

Purpose	Conditions
With your express consent	We disclose PHI to any person or service you explicitly authorize (e.g., your clinician).
Continuity of care	We may share PHI with other health-care providers involved in your treatment, but only as permitted by PHIPA and professional standards.
Service-provider (“agent”) support	PHI may be accessed by contracted vendors that host, maintain, or secure our software application. Each vendor signs a written agreement that: (i) restricts use to our stated purposes, (ii) enforces PHIPA-equivalent safeguards, and (iii) requires prompt breach notification. We do not allow agents to use PHI for their own marketing or analytics.
Legal or regulatory requirements	We disclose PHI when a court order, warrant, subpoena, or other statute compels us, or where PHIPA expressly authorises disclosure (e.g., to avert serious bodily harm).

Enforcement of our rights / fraud prevention	We may disclose PHI to establish, exercise, or defend legal claims, detect or prevent fraud or security threats, or investigate suspected unlawful activity, but always using the minimum PHI necessary, in accordance with the PHIPA.
Business transaction (succession)	If we merge, reorganise, or sell assets, PHI is transferred only if the recipient (a) is legally permitted to receive it, and (b) agrees in writing to use or disclose the PHI solely for completing the transaction and to continue protecting it in compliance with PHIPA.

We **never** sell PHI, and we do **not** use or disclose PHI for marketing, fundraising, or advertising without a separate, explicit opt-in consent.

Disclosures that involve only non-health Personal Data

Purpose	Typical recipients
Subsidiaries and affiliates	Internal group companies that support customer service, finance, or product development.
Business support vendors	Cloud-hosting providers, email delivery services, analytics platforms, payment processors, or professional advisers who help us operate the business. These vendors receive only the data necessary for their task and are bound by confidentiality and security obligations.
Business transaction	Transfer of non-health Personal Data to a successor entity in a merger, acquisition, or asset sale, subject to contractual privacy commitments.
Legal compliance and risk management	Courts, regulators, law-enforcement bodies, or insurers when we believe the disclosure is required to comply with law, enforce our terms, protect our rights or the safety of others, or investigate fraud.
Brand usage	With your permission, we may display your company name or logo on our website or marketing materials.
Other disclosures with consent	Any additional sharing you expressly approve at the time of collection.

Before any disclosure, whether PHI or Personal Data, we ensure that the recipient has appropriate administrative, technical, and physical safeguards to protect the information and that the disclosure complies with this Privacy Policy and applicable law.

10. Security of Personal Data and PHI

Security of Personal Data and PHI

We maintain a comprehensive information-security program designed to protect both Personal Data and PHI against loss, misuse, and unauthorised access or disclosure. Safeguards include encryption in transit and at rest, multi-factor authentication, strict role-based access controls, continuous intrusion monitoring, regular penetration testing, and audited backup and recovery procedures. Administrative measures, such as employee training, least-privilege policies, and vendor due-diligence reviews, complement these technical controls.

Despite these measures, no Internet transmission or electronic storage method can be guaranteed 100 percent secure. We therefore cannot promise absolute security, but we continually assess and enhance our defences to meet or exceed PHIPA requirements and relevant industry standards.

If PHI or Personal Data is lost, stolen, or accessed without authorization, we will notify affected individuals and the Information and Privacy Commissioner of Ontario at the first reasonable opportunity, as required by PHIPA s. 12(3), and will notify any other regulators where applicable.

The following sections 11 to 13 apply only to users in the specified jurisdictions and do not modify our obligations under PHIPA for Ontario users.

11. Your Data Protection Rights Under General Data Protection Regulation (GDPR)

If you are a resident of the European Union (EU) and European Economic Area (EEA), you have certain data protection rights, covered by GDPR. – See more at

- <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

We aim to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data.

If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please email us at admin@medmelanin.com.com.

In certain circumstances, you have the following data protection rights:

- (a) the right to access, update or to delete the information we have on you;
- (b) the right of rectification. You have the right to have your information rectified if that information is inaccurate or incomplete;

(c) the right to object. You have the right to object to our processing of your Personal Data;

(d) the right of restriction. You have the right to request that we restrict the processing of your personal information;

(e) the right to data portability. You have the right to be provided with a copy of your Personal Data in a structured, machine-readable and commonly used format;

(f) the right to withdraw consent. You also have the right to withdraw your consent at any time where we rely on your consent to process your personal information;

Please note that we may ask you to verify your identity before responding to such requests. Please note, we may not be able to provide Service without some necessary data.

You have the right to complain to a Data Protection Authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority in the European Economic Area (EEA).

12. Your Data Protection Rights under the California Privacy Protection Act (CalOPPA)

CalOPPA is the first state law in the United States to require commercial websites and online services to post a privacy policy. The law's reach stretches well beyond California to require a person or company in the United States (and conceivable the world) that operates websites collecting personally identifiable information from California consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals with whom it is being shared, and to comply with this policy. – See more at:

- <https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/>

According to CalOPPA we agree to the following:

(a) users can visit our site anonymously;

(b) our Privacy Policy link includes the word “Privacy”, and can easily be found on the page specified above on the home page of our website;

(c) users will be notified of any privacy policy changes on our Privacy Policy Page;

(d) users are able to change their personal information by emailing us at admin@medmelanin.com.

Our Policy on “Do Not Track” Signals:

We honor Do Not Track signals and do not track, plant cookies, or use advertising when a Do Not Track browser mechanism is in place. Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked.

You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

13. Your Data Protection Rights under the California Consumer Privacy Act (CCPA)

If you are a California resident, you are entitled to learn what data we collect about you, ask to delete your data and not to sell (share) it. To exercise your data protection rights, you can make certain requests and ask us:

(a) What personal information we have about you. If you make this request, we will return to you:

(i) The categories of personal information we have collected about you.

(ii) The categories of sources from which we collect your personal information.

(iii) The business or commercial purpose for collecting or selling your personal information.

(iv) The categories of third parties with whom we share personal information.

(v) The specific pieces of personal information we have collected about you.

(vi) A list of categories of personal information that we have sold, along with the category of any other company we sold it to. If we have not sold your personal information, we will inform you of that fact.

(vii) A list of categories of personal information that we have disclosed for a business purpose, along with the category of any other company we shared it with.

Please note, you are entitled to ask us to provide you with this information up to two times in a rolling twelve-month period. When you make this request, the information provided may be limited to the personal information we collected about you in the previous 12 months.

(b) To delete your personal information. If you make this request, we will delete the personal information we hold about you as of the date of your request from our records and direct any service providers to do the same. In some cases, deletion may be

accomplished through de-identification of the information. If you choose to delete your personal information, you may not be able to use certain functions that require your personal information to operate.

(c) To stop selling your personal information. We don't sell or rent your personal information to any third parties for any purpose. You are the only owner of your Personal Data and can request disclosure or deletion at any time.

Please note, if you ask us to delete or stop selling your data, it may impact your experience with us, and you may not be able to participate in certain programs or membership services which require the usage of your personal information to function. But in no circumstances, we will discriminate against you for exercising your rights.

To exercise your California data protection rights described above, please send your request(s) by one of the following means:

By email: admin@medmelanin.com

Your data protection rights, described above, are covered by the CCPA, short for the California Consumer Privacy Act. To find out more, visit the official California Legislative Information website. The CCPA took effect on 01/01/2020.

14. Analytics

We may use third party Service Providers (like Google Analytics, Firebase, etc.) to monitor and analyze the use of our Service.

15. CI/CD tools

We may use third party Service Providers (like GitHub) to automate the development process of our software application.

16. Payments

We may provide paid products and/or services within Service. In that case, we use third party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

17. Links to Other Sites

Our Service may contain links to other sites that are not operated by us. If you click a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

18. Minors' Privacy

Our Services are not intended for use by individuals under the age of 18 ("**Minors**").

We do not knowingly collect personally identifiable information from individuals under 18, unless authorized by their legal guardian. If you become aware that a Minor has provided us with Personal Data without explicit authorization of their legal guardian, please contact us. If we become aware that we have collected Personal Data and/or PHI from Minors without verification of the consent of their legal guardian, we shall take steps to remove that information from our servers.

19. Changes to This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our website or software application interface, prior to the change becoming effective and update "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

20. Contact Us

If you have any questions about this Privacy Policy, please contact us:

By email: admin@medmelanin.com.