SOVAKA HEALTH PRIVACY POLICY

Effective Date. This Privacy Policy is effective as of February 1, 2026.

OUR COMMITMENT TO PRIVACY:

This notice describes our Privacy Policy**.** Our privacy policy explains how Sovaka Health, LLC ("Sovaka") collects, uses, and protects the Personal Data obtained through the use of our Sovaka Health website ("Site") and the public and professional in health portals, webinars, and related digital health services available through the Site (collectively, "Services"). Through the Services we provide a unified and comprehensive digital health solution is designed to enhance health outcomes by blending human touch may with AI support. By visiting the Site or using any of our Services, you agree that your Personal Data will be handled as described in this Privacy Policy. Your use of our Site or Services, and any dispute over privacy, is subject to this Privacy Policy and our Terms of Use, including its applicable limitations on damages and the resolution of disputes. The Sovaka Terms of Use are incorporated by reference into this Privacy Policy.

In addition to this Privacy Policy, we have internal policies and practices designed to keep your Personal Data secure and to ensure that information about you is only used consistent with this Privacy Policy. We have privacy and security teams that are committed to ensuring that your Personal Data is safe and handled properly.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our Site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features in an effort to prevent loss, theft and unauthorized access, use and disclosure.

CHANGES TO PRIVACY POLICY:

Sovaka reserves the right to change this Privacy Policy from time to time as it sees fit and your continued use of the Service will signify your acceptance of any adjustment to this Privacy Policy. If there are any changes to our Privacy Policy, we will announce that these changes have been made on our home page and on other key pages on our Services. If there are any changes in how we use our users' Personal Data, notification by e-mail will be made to those affected by this change. Any changes to our Privacy Policy will be posted on our Services 30 days prior to these changes taking place. You are therefore advised to re-read this Privacy Policy on a regular basis.

WHAT INFORMATION IS COLLECTED:

We collect information about you directly from you and from third parties, as well as automatically through your use of our Site or Services.

(a) Information We Collect Directly From You.

For all Users, if you wish to use the Services, you will be required to create an account (each an "Account"). We may collect the following information, including Protected Health Information ("PHI") through the Account registration process, all of which is defined as "Personal Data":

Individual Users:

- Email address, approximate location
- PHI: e.g., health diaries, profiles, conditions
- Credit card, bank account or other payment information
- Photos or phone numbers
- IP address

Organization or Business Entity Users:

- Organization's name and tax identification number
- Mailing address, phone number, email address
- Name of authorized User creating the Account
- Any additional information that may be requested from time to time

Healthcare User:

- Full name, mailing address, phone number
- Valid professional license details
- Any additional information that may be requested from time to time

(b) Information We Collect Automatically. We may automatically collect information about your use of our Services through cookies, web beacons, and other technologies. We combine this information with other information we collect about you. Such information may include:

- domain name;
- your browser type and operating system;
- web pages you view; links you click; your IP address;
- the length of time you visit our Site and or use our Services;
- the referring URL, or the webpage that led you to our Site.

(c) **Information we obtain from other sources.**
Other third-party services may be able to collect information about you, including information about your activity on our Site, and they may notify your connections on the third-party services about your use of the Services, in accordance with their own privacy policies. We may receive the information described in this Privacy Policy from third party services, such as analytics providers.

HIPAA COMPLIANCE AND NOTICE OF PRIVACY PRACTICES:

Sovaka may receive, create, maintain, or transmit PHI on behalf of Users. We comply with HIPAA and related laws, implementing safeguards to protect the privacy and

security of PHI. We only use or disclose PHI as necessary to provide our Services, and any subcontractors or Service Providers are required to uphold the same protections.

If you are a User whose PHI we handle through a healthcare User, you have rights under HIPAA. These rights and our obligations are detailed in the Notice of Privacy Practices (NPP) provided by the Covered Entity. For more information or to request a copy of the NPP, please contact the healthcare provider or entity through which your PHI is managed.

PAYMENT TERMS:

When you make a purchase through our Services, we collect certain payment details necessary to process your transaction. This may include your name, billing address, and payment method information. Payments are processed securely by third-party payment processors, which may include PayPal, Google Pay or a credit card processor. We do not store or have access to your complete credit card or bank account details. We use this Personal Data solely for the purpose of completing your transaction, preventing fraud, and complying with legal or regulatory requirements.

HOW AND WHEN THE INFORMATION IS USED:

Currently, we may use your Personal Data for the following purposes:

a. To respond to host and manage webinars.
b. To personalize health tools and artificial intelligence insights.
c. To provide our Services to you, to communicate with you about your use of our Services, to respond to your inquiries, and for other customer service purposes.
d. To tailor the content and information that we may send or display to you, to offer location customization, and personalized help and instructions, and to otherwise personalize your experiences while using the Site.
e. For marketing and promotional purposes. For example, we may use your information, such as your email address, to send you news and newsletters, or to otherwise contact you about information or job openings we think may interest you.
f. To better understand how users access and use our Site and Services, both on an aggregated and individualized basis, in order to improve our Site and Services and respond to user desires and preferences, and for other research and analytical purposes.
g. To protect our own rights and interests, such as to resolve any disputes, enforce our Terms of Use or to respond to legal process.

HOW WE SHARE YOUR INFORMATION:

We may share your information, including Personal Data, as follows:

Service Providers. We will not sell, trade, or rent your Personal Data to others. However, we do provide some of our Services through contractual arrangements made with affiliates, service providers, partners and other third parties ("Service Providers"). Our Service Providers include health care providers, administrators for clinical

collaboration, payment processors, or third-party processors under signed HIPAA Business Associate Agreements.

We and our Service Partners may need to use some Personal Data in order to perform tasks between our respective sites, or to deliver services to you.

We may also share information in the following circumstances:

a. **Business Transfers.** If we are acquired by or merged with another company, if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding, we may transfer the information we have collected from you to the other company.
b. **In Response to Legal Process.** We also may disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a court order or a subpoena.
c. **To Protect Us and Others.** We also may disclose any information we collect from you where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Use or this Privacy Policy, or as evidence in litigation in which we are involved.
d. **Aggregate and De-Identified Information.** We may share aggregate or de-identified information about users with third parties for marketing, advertising, research or similar purposes.

BUSINESS ASSOCIATE COMPLIANCE

Sovaka may receive or process Protected Health Information ("PHI") on behalf of Users. We comply with HIPAA and related laws, using appropriate safeguards to protect the privacy and security of PHI. We only use or disclose PHI as necessary to provide our Services, and we require any subcontractors to uphold the same protections. In the event of a security incident or unauthorized access affecting PHI, we will notify the affected User promptly.

HOW WE PROTECT YOUR INFORMATION:

To protect your Personal Data, including PHI, we take reasonable precautions and follow industry standard TLS 1.2 or higher end-to-end encryption of data in transit and at rest using AES-256 encryption, to make sure it is not inappropriately lost, misused, accessed, disclosed, altered or destroyed. If you directly provide us with any Personal Data, the information is encrypted using industry standard protections in our database. We also have strict internal access controls (including multi-factor authentication for all healthcare provider Accounts and administrative access) and run periodic security audits to ensure compliance.

All information we collect may be stored as follows, unless we receive a request by you to remove such information or you choose to terminate our access to your Account:

- **Any PHI or other sensitive information:** Minimum of 6 years.
- **Billing/transactional data**: 7 years.

- **Account Personal Data**: Retained while your Account remains active; deleted or anonymized upon request or inactivity.

- **De-identified/aggregated data**: May be retained indefinitely for research, analytics, or public health purposes.

Although we have implemented commercially reasonable precautions to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, please be aware that despite our best efforts, no data security measures can guarantee 100% security. You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

CONTACT AND LOCATION:

Please be advised the data processing activities take place in the United States, outside the European Economic Area. Data may also be transferred to companies within the United States, but will only be done so in a manner that complies with the EU's General Data Protection Regulation or GDPR. The location where the data processing activities take place is as follows:

All data is stored within either Supabase, Microsoft forms, Vercel, **Amazon Web Services** ("AWS") or similar using their **Services infrastructure**, hosted in **U.S.-based data centers** or data centers based on your location that comply with regulations. We may use the following or similar

- **HIPAA-eligible services** provided by AWS, such as AWS HealthLake and Amazon S3, for storing and managing sensitive health data.
- Services provided by Vercel, such as a service provider or data processor and implement security measures to protect the data
- Microsoft Forms –
  - Users in EU member countries have their Personal Data stored in the Macro Region Geography 1 - EMEA.
  - For Users in Australia, Microsoft Forms data is stored at rest in Australia for all new Users using Forms and existing Users that have not previously used Forms.
  - All other Users have their customer Personal Data stored in the United States.
- Supabase – all personal data stored at its US-West-1 data center or similar
- **U.S.-based data centers** that comply with healthcare regulations.

CAN-SPAM ACT AND OPTING OUT OF EMAILS:

The CAN-SPAM Act is a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them, and spells out tough penalties for violations. We collect your email address in order to:

- Send information, respond to inquiries, and/or other requests or questions.
- We may also send you additional information related to your Account or our Services.
- Market to our mailing list, if you provide us with such consent.

To be in accordance with CAN-SPAM we agree to the following:

- NOT use false, or misleading subjects or email addresses
- Identify the message as an advertisement in some reasonable way
- Include the physical address of our business or site headquarters
- Monitor third party email marketing services for compliance, if one is used.
- Honor opt-out/unsubscribe requests quickly
- Allow users to unsubscribe by using the link at the bottom of each email

We may send periodic promotional or informational emails to you. You may opt-out of such communications by following the opt-out instructions contained in the email. Please note that it may take up to 10 business days for us to process opt-out requests. If you opt-out of receiving emails about recommendations or other information we think may interest you, we may still send you emails about your Account or any other transactional or Service-oriented request.

OUR USE OF COOKIES AND OTHER TRACKING MECHANISMS:

Cookies. Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate our Site and Services, while others are used to enable a faster log-in process or to allow us to track your activities at our Site and Service. Cookies do not record or store any Personal Data. If you want, you can prevent the use of cookies, but then you may not be able to use our Services as we intend. To proceed without changing the options related to cookies, simply continue to use our Services. We may utilize third-party cookies via Google Analytics, Squarspace, LinkedIn and other Services Providers.

Example Squarespace and LinkedIn are two Service Providers that may place cookies on our Site.

WHAT ARE THE DIFFERENT TYPES OF COOKIES AND HOW DO WE USE THEM?

a) *Essential:* These are cookies which are essential for the running of our Site. Without these cookies, parts of our Site would not function. These cookies do not track where you have been on the internet and do not gather information about you that could be used for marketing purposes.

   Examples of how we may use essential Cookies include:

   - Setting unique identifiers for each unique visitor, so that user numbers can be analyzed.

b) *Functional:* These cookies are used to remember your preferences and login information on our Site and to provide enhanced, more personal features. The information collected by these cookies is usually anonymized, so we cannot identify you personally. Functional cookies do not track your internet usage or gather information which could be used for selling advertising.

   Examples of how we may use functional Cookies include:

   - Storing language preferences, autofill forms or accessibility preferences
   - Gathering data about visits to our Site, including numbers of visitors and visits, length of time spent on the Site, or where visitors have come from.

c) *Third Party Cookies*: You may notice on some pages of our Site that cookies have been set that are not related to us. When you visit a page with content embedded from these third-party service providers, they may set their own cookies on your device. We do not control the use of these third-party cookies and cannot access them due to the way that cookies work, as cookies can only be accessed by the party who originally set them. Please check the third-party websites or mobile applications for more information about these cookies.

d) *Analytical Performance*: Analytical performance cookies are used to monitor the performance of our Site, for example, to determine the number of page views and the number of unique users our Site has. We use this information to improve user experience or identify areas of the Site which may require maintenance. The information is anonymous (i.e. it cannot be used to identify you and does not contain Personal Data such as your name and email address) and it is only used for statistical purposes.

   Examples of how we may use analytical cookies include:

   - Measuring Users' behavior
   - Analyze which pages are viewed and how long for and which links are followed to better develop our Site.

e) *Disabling Cookies:* Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The Help portion of the toolbar on most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to

disable cookies altogether. If you choose to refuse, disable, or delete cookies, some of the functionality of our Site may no longer be available to you. Without this information, we are not able to provide you with all the requested services, and any differences in services are related to your information.

- Some browsers transmit "do-not-track" signals to websites. Because of differences in how browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. We currently do not take action in response to these signals.

f) *Clear GIFs, pixel tags and other technologies:* Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (a.k.a. web beacons, web bugs or pixel tags), in connection with our Site and Services to, among other things, track the activities of Site visitors, help us manage content, and compile statistics about Site usage. We and our third party service providers also use clear GIFs in HTML emails to our customers, to help us track email response rates, identify when our emails are viewed, and track whether our emails are forwarded.

g) **Log Data:** Like all websites, this Services also makes use of log files that store automatic information collected during user visits. The different types of log data could be as follows:
   - internet protocol (IP) address
   - type of browser and device parameters used to connect to the Services;
   - name of the Internet Service Provider (ISP);
   - date and time of visit;
   - web page of origin of the user (referral) and exit;
   - possibly the number of clicks.

THIRD PARTY ANALYTICS:

We use automated devices and applications, such as Google Analytics, to evaluate usage of our Site. We also may use other analytic means to evaluate our Services. We use these tools to help us improve our Services, performance and user experiences. These entities may use cookies and other tracking technologies to perform their services. We do not share your Personal Data with these third parties.

BREACH NOTIFICATION:

Sovaka takes the security of your information seriously. In the event of a data breach affecting Personal Data, including PHI. we will respond promptly in accordance with applicable laws, including:

- **HIPAA** – We will notify affected Covered Entities without unreasonable delay and in no case later than the timeframes required under HIPAA regulations.
- **GDPR** – For EU users, we will notify the relevant supervisory authority of a personal data breach within 72 hours of becoming aware of it, and affected individuals where required.
- **U.S. State Laws** – We will comply with any additional state-specific notification requirements, including notifying affected individuals as required by law.

Notifications will include, to the extent known, the nature of the breach, the categories of data affected, steps we are taking to mitigate harm, and contact information for further inquiries.

THIRD-PARTY LINKS:

When you click on links on our Site, they may direct you away from our Site. We are not responsible for the privacy practices of other websites or mobile applications and encourage you to read their individual privacy policies. If you visit a third-party website or mobile application link from our Site, you do so at your own risk.

HOW YOU CAN ACCESS YOUR INFORMATION:

Although we describe much of the following processes throughout this Privacy Policy, please do not hesitate to email us at Supportmvp@sovakahealth.onmicrosoft.com to receive the following information:

What Personal Data pertaining to you is being processed by us
Why this information is being processed
Who has access to this Personal Data about you
How this Personal Data is being used in automated decisions
What processes are using this information

CHILDREN:

We do not intentionally collect or maintain Personal Data from persons under the age of 18. If we determine upon collection that a user is under this age, we will not use or maintain his/her Personal Data without the parent/guardian's consent. If we become aware that we have unknowingly collected Personal Data from a child under the age of 18, we will make reasonable efforts to delete such Personal Data from our records. We also recommend that parents monitor their children's Internet activities and learn and employ software or other tools that can help their children enjoy their online experience without compromising their personal safety or allowing them to use the Internet in a manner inconsistent with their parent/guardian's preferences

If we ever provide Services to users under 18, or if a parent believes their child under 18 has provided information, we will:

1. **Request Parental Consent** – Before collecting any Personal Data, we will obtain verifiable parental consent through a method such as:
    - Email or postal consent forms;
    - Credit card verification or other online verification methods; or
    - Other reliable methods approved under COPPA.
2. **Parental Access and Control** – Parents can review, request deletion, or refuse further collection of their child's information by contacting us at Supportmvp@sovakahealth.onmicrosoft.com.

INTERNATIONAL DATA TRANSFER FOR RESIDENTS OF THE EUROPEAN UNION, SWITZERLAND OR THE UNITED KINGDOM:

EU data protection law through GDPR or the UK GDPR and UK Data Protection Act makes a distinction between organizations that process Personal Data for their own purposes (known as "data controllers") and organizations that process Personal Data on behalf of other organizations (known as "data processors"). If you have a question or complaint about how your Personal Data is handled, these should always be directed to the relevant data controller since they are the ones with primary responsibility for your Personal Data.

If you are located in the European Union, the United Kingdom, or another jurisdiction where the General Data Protection Regulation (GDPR/UK GDPR) applies, you have the following rights regarding your Personal Data:

- Right of Access: You may request confirmation of whether we process your Personal Data and obtain a copy.
- Right to Rectification: You may request correction of inaccurate or incomplete Personal Data.
- Right to Erasure ("Right to be Forgotten"): You may request deletion of your Personal Data, subject to legal or regulatory exceptions.
- Right to Restrict Processing: You may request that we limit the processing of your Personal Data under certain conditions.
- Right to Data Portability: You may request a copy of your Personal Data in a structured, commonly used, machine-readable format and transmit it to another controller.
- Right to Object: You may object at any time to processing of your Personal Data carried out on the basis of legitimate interests or for direct marketing purposes.
- Right to Lodge a Complaint: You may lodge a complaint with your local Data Protection Authority if you believe your rights have been infringed. An explanation of the process is available at: https://www.edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

There may be circumstances where we are not legally required to comply with your request because of the laws in your jurisdiction or because of exemptions provided for in data protection legislation. If you have a complaint about how we handle your Personal Data, please get in touch with us as at Supportmvp@sovakahealth.onmicrosoft.com to receive further clarification. If you are not happy with how we have attempted to resolve your complaint, you may contact the relevant data protection authority.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our App, Site or the Services; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features in an effort to prevent loss, theft and unauthorized access, use and disclosure.

a) **Legal Grounds for Processing your Personal Data**

The GDPR requires us to tell you about the legal ground we're relying upon to process any Personal Data about you. The legal basis for us processing your Personal Data for the purposes set out in this Privacy Policy will typically be because:

- you provided your explicit consent;
- it is necessary for our contractual relationship;
- the processing is necessary for us to comply with our legal or regulatory obligations; and/or
- the processing is in our legitimate interest for the purpose of the Services (for example, to protect the security and integrity of our systems and to provide you with customer service, etc.).

b) **Sovaka Health as a Data Controller**

Sovaka Health will act as a data controller concerning Personal Data. For example, if you create an Account with us, make a purchase or access the message boards or forums, Sovaka Health will be a data controller for the Personal Data you provide as part of your Account.

We will also be a data controller of the Personal Data we may obtain through the use of the Services or our Services. We use this to conduct research and analysis to help better understand and serve users of the Services as well as to improve our Services.

c) **Transfers of Personal Data**

Sovaka is a United States company. If you are located outside the United States and choose to provide information to us, Sovaka transfers and stores Personal Data to the United States for processing. The U.S. may not have the same data protection laws as the country in which you initially provided the information. When we transfer your information to the U.S., we will protect it as described in this Privacy Policy. When transferring Personal Data outside of the EU, EEA, Switzerland, or the United Kingdom, we use lawful transfer mechanisms such as the European Commission's Standard Contractual Clauses (SCCs), or rely on the EU–U.S. Data Privacy Framework where applicable. These safeguards ensure that your Personal Data continues to receive adequate protection in line with GDPR standards. By visiting the Site, using our Services or providing Sovaka with any information, you fully understand and unambiguously consent to this transfer, processing and storage of your information in the United States.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our Site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features in an effort to prevent loss, theft and unauthorized access, use and disclosure.

By visiting the Site, using our Services or providing Sovaka Health with any information, you fully understand and unambiguously consent to this transfer, processing and storage of your information in the United States.

We retain your Personal Data for as long as necessary to provide you with our Services or for other important purposes such as complying with legal obligations, resolving

disputes, and enforcing our agreements. Sovaka Health may retain non-Personal Data for as long as necessary for the purposes and uses described in this Privacy Policy, including as necessary for Sovaka Health to pursue legitimate and lawful business interests.

More specifically, we separate our retention of various Personal Data and non-Personal Data as follows:

- **Any PHI or other sensitive information:** Minimum of 6 years.
- **Billing/transactional data**: 7 years.
- **Account Personal Data**: Retained while your Account remains active; deleted or anonymized upon request or inactivity.
- **De-identified/aggregated data**: May be retained indefinitely for research, analytics, or public health purposes.

USERS IN BRAZIL:

LEGAL BASIS FOR PROCESSING YOUR INFORMATION

Depending on what information we collect from you and how we collect it, we process your information for the following reasons:

- In order to administer our contractual relationship, including setting up your requested Services, payments, renewals and processes;
- Because it is in our legitimate interest to run a successful and efficient business and provide you with the Services and other useful content;
- In order to fulfill any legal obligations we may have to collect this information from you; and/or
- Because you have provided your explicit consent for us to do so.

SHARING WITH THIRD PARTY SERVICE PROVIDERS AND VENDORS

Occasionally, we enter into contracts with selected third parties to assist us in servicing you (for example, providing you with customer service, fraud detection and deterrence or access to advertising assets and providing us with information technology and storage services) or to assist us in our own marketing and advertising activities (including providing us with analytic information and search engine optimization services). Additional information about certain third-party service providers we share Personal Data with is available here. Our contracts with such third parties prohibit them from using any of your Personal Data for any purpose beyond the purpose for which it was shared.

DATA TRANSFERS

In order for us to provide the Services to you and comply with our legal obligations, Personal Data you provide to us and information we collect about you, your usage and devices will be transferred to, stored and processed in the United States. Your

information may also be processed by staff operating outside of the United States who work for one of our Third Party Service Providers. We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this Brazil Privacy Addendum.

COOKIES

You can select your cookie preferences upon your first visit to our Site. If you choose to change your preferences, you may do so at any time by clicking the “Cookie Preferences” link in the footer of our website homepage.

When you opt out of cookies, you will be opted out of all non-required cookies. You cannot opt out of required cookies because these cookies and tracking technologies are required to help our websites work correctly. These cookies allow you to navigate our Services and use essential features, including secure areas and authentication orders.

YOUR PRIVACY RIGHTS

As a user located in Brazil, you may be able to exercise the following rights with respect to your Personal Data that we have collected, subject to certain limitations:

The right to ask that we provide confirmation of the existence of data processing	You have the right to ask that we provide confirmation of the existence of the processing of your personal data.
The right to access your information	You have the right to access the personal data we hold about you and certain information about how we use it and who we share it with including information about any public and private entities we have shared your personal data with.
The right to correction	You have the right to ask us to update or correct personal information if it is inaccurate, incomplete or out-of-date data.
The right to request deletion	You have the right to request the deletion of personal information we have collected from you, subject to certain exceptions.
The right to request anonymization and blocking	You have the right to ask us to anonymize, block, or delete unnecessary or excessive data or data that is not being processed in compliance with the LGPD.
The right to data portability	You have the right to ask us to port your data to another service or product provider.
The right to ask information about the possibility of denying consent	You have the right to ask us to provide information about the possibility of denying consent for the processing of your personal data and the consequences of such denial.

To exercise your rights under the LGPD, please submit a request to us by:

- Sending an email to Supportmvp@sovakahealth.onmicrosoft.com

We will need to verify your identity before processing your request. In order to verify your identity, we will generally require the matching of sufficient information you provide us to the information we maintain about you in our systems.

COMPLAINTS

If you have any questions about this Brazil Privacy Addendum or our data handling practices, or you wish to make a complaint, you may contact our Data Protection Officer at Supportmvp@sovakahealth.onmicrosoft.com.

In addition to the rights outlined above, where the Lei Geral de Proteção de Dados (LGPD) applies, you may:

- Ask that we provide confirmation of the existence of the processing of your personal data.
- Access the personal data we hold about you and certain information about how we use it and who we share it with including information about any public and private entities.
- Request the deletion of Personal Data we have collected from you, subject to certain exceptions.
- Ask us to anonymize, block, or delete unnecessary or excessive data or data that is not being processed in compliance with the LGPD.
- Ask us to provide information about the possibility of denying consent for the processing of your personal data and the consequences of such denial.

CALIFORNIA AND VIRGINIA RESIDENTS:

If you live in California or Virginia, you have certain additional rights regarding your Personal Data. This includes the right to request:

- **Right to Know**: You may request that we disclose the categories of Personal Data we collect, the purposes for which we use it, and the categories of third parties with whom we share it.
- **Right to Access and Data Portability**: You may request a copy of your Personal Data in a portable format.
- **Right to Correct**: You may request correction of inaccurate Personal Data.
- **Right to Delete**: You may request that we delete your Personal Data, subject to certain legal exceptions.
- **Right to Opt-Out of Sale or Sharing**: Sovaka Health does not sell Personal Data. However, we may share limited data with advertising or analytics partners (e.g., cookies, pixels) for cross-context behavioral advertising.
- **Right to Non-Discrimination**: Exercising your privacy rights will not result in different prices, rates, or quality of Services.

These rights are not absolute, and in some circumstances, Sovaka may decline to satisfy your request. For example, if we are unable to verify your identity or if your

request impacts other people's privacy rights, we may deny your request to exercise these rights. We may also deny your request when Sovaka has the legal right to do so, such as when we have an ongoing business relationship with you, an ongoing need to use the information for purposes outlined in this Privacy Policy, or we are legally required to retain your Personal Data. If Sovaka denies your request to exercise your privacy rights, we will tell you why we are denying the request and provide you with information about how to appeal this decision.

If you choose to exercise your privacy rights, we will not charge you different prices or provide a different quality of services unless those differences are related to your Personal Data.

The categories of Personal Data we collect and the purpose of said collection is as follows:

Category of Data	Purpose of Use	Shared With
Personal Identifiers (e.g., name, email, phone)	To create and manage your account, provide services, and communicate with you	Authorized service providers, Covered Entities you interact with
Health Information / PHI (if provided via a Covered Entity)	To perform services on behalf of healthcare clients in compliance with HIPAA	Healthcare clients (Covered Entities), authorized subcontractors bound by HIPAA
Usage Data (e.g., logs, analytics)	To improve our services and detect technical issues	Internal team, service providers supporting analytics and infrastructure
Payment or Billing Information	To process payments and manage billing	Payment processors and financial institutions

How to Submit a Request for Access, Correction, or Deletion of Personal Data.

If you would like to submit a request about your Personal Data, we encourage you to do so by emailing us at Supportmvp@sovakahealth.onmicrosoft.com.

Sovaka Health does not sell Personal Data in exchange for money. However, we may allow certain third-party partners (such as advertising networks, social media platforms, and analytics providers) to collect information from our Site and Services through cookies, pixels, and similar technologies. Under California law, this may be considered "sharing" Personal Data for cross-context behavioral advertising.

Opt-Out of Sale or Sharing

You have the right to direct us **not to sell or share your Personal Data**. You may exercise this right at any time by:

- Adjusting your cookie preferences through the cookie banner shown when you first visit our Site; or
- Sending us an email at **Supportmvp@sovakahealth.onmicrosoft.com** with the subject line “Do Not Sell or Share Request.”

When you opt out, Sovaka Health will stop sharing your Personal Data with third parties for cross-context behavioral advertising. Please note that opting out does not disable all cookies. Essential cookies (needed for our Site to function properly) will continue to operate.

Authorized Agents

You may also designate an authorized agent to submit an opt-out request on your behalf. To do so, we may require you to provide written authorization for the agent or verify your own identity directly with us.

After you submit the request, you will be asked to verify your email address and may also be asked to provide additional information to verify your identity. Sovaka will attempt to verify your identity by asking for information that correlates with the information that we have previously collected about you. If this is not possible, Sovaka may request you submit additional information for verification, such as proof of residency or redacted government-issued identification.

You may also designate an authorized agent to make a request on your behalf. To designate an authorized agent, you must provide Sovaka with written permission for the agent to make the request on your behalf or provide us with an executed power of attorney. You will also be required to submit both your and the authorized agent’s valid government-issued identification.