

Privacy Notice

Effective Date: July 2, 2021

Last Revised Date: July 23, 2026

Redi.Health Inc., a Delaware corporation (“Redi.Health”, the “Company”, “our” “us,” and/or “we”) respects the privacy of its users (“User” or “you”) of its platform, including website, mobile application, embedded interface, partner-facing experience, and SMS or other messaging channels, and any related features, functionality, and content that we make available through any of those access points (collectively, the “Platform”), and is committed to protecting your Personal Data (defined below). For convenience, references in this Privacy Notice to the “Mobile Application” mean the mobile application component of the Platform.

We believe that you have a right to know our practices regarding the Personal Data we may collect, use, and disclose about you when you use our Platform. Please read the following carefully to understand our views and practices regarding information about you (“Personal Data” or “Personal Information”) and regarding how we treat it. This Privacy Notice, along with our Terms of Service (sometimes called the “Terms”), constitute an agreement between you and us while you are accessing and using our Platform to engage our services (“Services”) and should be read carefully. Please be advised that the practices described in this Privacy Notice apply to the information, including Personal Data, gathered through our Platform and/or the Services, information that you submit to us, and we may collect from third parties.

In summary, when using the Platform, we may collect some Personal Data, in order to provide you with the Services and to show value to our third-party business partners and service providers, including, the representatives of pharmaceutical manufacturers, medical insurance companies, hub companies, pharmaceutical services providers, hospitals (including nurses), or another medical institutes (collectively, “Partners”) who may provide some of the Services. If you engage with one of our Partners, we may share Personal Data with them. We also allow you to interact with Partners within the Platform, where in such case Personal Data will be shared with Partners.

BY ACCESSING OR USING ANY PART OF THE PLATFORM, YOU AGREE THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO BE BOUND BY THIS PRIVACY NOTICE, WHICH DESCRIBES HOW WE COLLECT, USE AND DISCLOSE YOUR DATA AND THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO BE BOUND BY OUR PRIVACY NOTICE AND OUR TERMS, WHICH CONTAINS AN ARBITRATION AGREEMENT, LIABILITY LIMITATIONS, AND A CLASS ACTION WAIVER ALL OF CLAMS THAT ARE INCORPORATED INTO THIS PRIVACY NOTICE, AND YOU CONSENT TO THE TERMS. IF YOU DO NOT AGREE TO BE SO BOUND, YOU MAY NOT ACCESS OR USE THE PLATFORM OR ANY OF OUR SERVICES.

About this Privacy Notice

This Privacy Notice applies when you use our Platform and describes our practices on the collection, use and disclosure of Personal Data collected from you and other users. This Privacy

Notice explains our online information practices and the choices you can make about the way your Personal Data is collected and used in connection with our Platform.

Eligibility

The Platform contains information about products that are approved and cleared for use in the United States, including Puerto Rico. The Platform is limited to users residing in the United States of America, including Puerto Rico. If you reside outside of the United States of America, please do not use the Platform.

Accounts on the Platform are held only by individuals who are at least eighteen (18) years old and who have the legal capacity to enter into our Terms of Service. Minors and individuals who otherwise lack legal capacity do not register or hold their own Accounts. A parent, legal guardian, person standing in loco parentis, or other authorized personal representative under applicable law (each, a “Caregiver”) may register and maintain an Account through which the Caregiver manages profiles for individuals for whom the Caregiver is authorized to act (each, a “Dependent”), as further described in our Terms of Service. Personal Data about a Dependent enters the Platform through the Caregiver, who is responsible for providing any consent or authorization required for the collection, use, and disclosure of the Dependent’s information. See the “Children’s Privacy” section below for additional information about how we treat data concerning children.

Who Are We?

Redi.Health is a company organized under the laws of Ohio, USA, with offices at 80 East Rich Street, Suite 660, Columbus, Ohio, United States. Individuals wishing to contact us about data protection issues may do so by emailing us at support@Redi.Health or by writing to us at Privacy Officer, 80 East Rich Street, Suite 660, Columbus, Ohio 43215.

What Data Do We Collect About You?

During the preceding 12 months, we have collected and/or disclosed for our business purposes the following categories of Personal Data:

- **Identifiers**, such as your name, contact information, email address, year of birth, and online identifiers.
- **Internet and electronic network activity information**, such as information about your interactions with our Services.
- **Non-personally identifiable data**, which consists of technical information and behavioral information that does not pertain to a specific individual, such as a sponsor code that was given to you from a pharmaceutical manufacturer to allow you to input information into the Platform, information from integrated fitness wearables, responses to in-Mobile Application questions, and other information.
- **Caregiver contact information**, which includes identifiers and contact details of a Caregiver (defined below).
- **Technical data that might be de-anonymized**, such as the type and version of your device and its operating system, the type of browser, screen resolution,

keyboard language, Wi-Fi connectivity, the type and name of your device and/or browser, your mobile operator service provider, IP address, etc. Additional information that may include your click-stream on the Platform, your activities on the Platform including time spent on various screens of the Platform and additional information of a similar nature. While it is not specifically personally identifiable, it may be reverse-engineered to be identifiable and therefore is considered Personal Data.

- **Demographic information**, such as gender and age.
- **Geolocation**, such as your approximate location (“Geolocation”) while using the Mobile Application.
- **Sensitive information**, includes information that overlaps with data in other categories listed above, and may additionally include information concerning your medical condition, including medications, pictures/visuals of your medical condition, allergies, symptoms, medications and medication adherence, conditions, allergies, information about your diet, information about your weight, information about your fitness activities, information about any swelling you may be experiencing or experienced, Geolocation, and age (“Sensitive Information”).

How We Collect Personal Data?

1. **Information that you provide through communications with us, including the registration process, and when you provide feedback or need support.** We may ask you to provide Personal Data in order to provide you with the services in connection with our Platform. Personal Data may be provided to us as part of any communications you have with us, by any means, including by approaching our customer services, or approaching us in order to receive technical support, including by phone (such information may include marketing and communication data that includes your preferences in receiving marketing from us and your communication preferences). We may record such calls for quality assurance purposes and in order to improve our services and, if we do, we will provide you such notice at the time of the call. We also periodically supplement the Personal Data we collect from you by obtaining personal or non-personal information about you or another person from other businesses, business partners, contractors, and other third parties (including, without limitation, Partners). We also collect information when you contact us and provide us with feedback relating to the Platform either through the Platform or via email. Once your feedback is received by us, our representative may contact you for further communication. We may collect medical and insurance related forms you may fill out from within the Platform. We may collect various kinds of content, information and materials that you may upload, publish and/or share with others within the Platform, such as in the emails, chats, photos, documents, any information input into the Platform, etc. (the “User Generated Content”). We may collect medical and insurance related forms you may fill out from within the Platform.

As you use the Platform and Services, you may choose to disclose to us medical, health and biometric information via the Platform’s “My Redi Record,” “Medication Tracker,” “Symptom Tracker,” “Diet Tracker,” “Weight Tracker,” “Activity Tracker,” “Conditions,” “Allergies,” and “Health Tracker.”

We only collect Sensitive Information with your consent.

2. **Information collected from a Caregiver.** We collect Dependent information from the Caregiver and connected providers/partners. Dependents do not receive login credentials for Platform access. Where we act as a Business Associate to a Covered Entity, we follow the Covered Entity's determinations about a personal representative under 45 C.F.R. § 164.502(g).

3. **Information collected from your computer or electronic device.** We collect information about your computer or other electronic device when you interact with our Platform and use our Services. This information includes your non-personally identifiable data, described above, and is provided by tracking technologies, such as cookies, web-beacons, pixel tags, software development kits (SDKs) embedded in our Mobile Application, mobile advertising identifiers (such as Apple IDFA and Google's Android's Android Advertising ID), server logs, and similar technologies (collectively, "Tracking Technologies"). We use Tracking Technologies for purposes such as authenticating users and maintaining sessions, remembering your preferences, measuring how the Platform is used and improving its performance, debugging and security monitoring, and (where applicable) attributing the source of traffic to the Platform. We do not deploy Tracking Technologies that transmit Protected Health Information ("PHI") or other Sensitive Information to third-party advertising networks for marketing purposes, and we do not use Tracking Technologies to engage in "cross-context behavioral advertising" as defined under U.S. state consumer privacy laws. The specific Tracking Technologies and analytics providers we use, and their categories, are described in our Cookie Policy below and may change from time to time as we update our service-provider arrangements.

Cookie Policy

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. Cookies are small text files that are stored on your computer or device when you visit certain online pages that record your preferences. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. When you use the Mobile Application, similar functionality is provided by SDKs and mobile identifiers rather than browser cookies, but the categories described below apply equally where the corresponding capability exists in the Mobile Application. Because we respect your right to privacy, you can choose not to allow some types of cookies. However, blocking some types of cookies may impact your experience of the Platform and our Services.

- **Strictly Necessary Cookies.** These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work.
- **Performance Cookies.** These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the

site. If users do not allow these cookies we will not know when users have visited our site and will not be able to monitor its performance.

- **Functional Cookies.** These cookies and similar technologies allow the Platform to remember choices you have made (such as your language, region, or display preferences) and to provide enhanced or personalized features. The information collected by these technologies may be anonymous, but if you do not accept them, some functionality may be limited.
- **Mobile Application SKDs and Device Identifiers.** When you use the Mobile Application, we and our service providers use software development kits (SDKs) and may access mobile device identifiers (such as Apple's IDFA and Google's Android Advertising ID, where you have not limited their use through your device settings) for analytics, crash reporting, performance monitoring, and security purposes. These technologies serve a function comparable to Strictly Necessary, Performance, and Functional cookies on the website. You can limit the use of mobile advertising identifiers through your device's privacy setting (for example, "Allow Apps to Request to Track" on iOS or "Reset Advertising ID" on Android).

We do not use Tracking Technologies for cross-context behavioral advertising or to engage in "targeted advertising" as those terms are defined under U.S. state consumer privacy laws. We also do not place third-party advertising or marketing Tracking Technologies on pages or screens of the Platform where authenticated users are providing or viewing their Personal Health Information. You can manage browser cookies through your browser settings; you can manage mobile device identifiers through your device's privacy setting; and, where required by applicable law, we recognize Global Privacy Control (GPC) signals sent by your browser as required to opt out of any "sale" or "sharing" of your Personal Information.

Why do we collect, use, and disclose Personal Data?

We collect and use the Personal Data we collect about you in the categories set forth above to:

- Enhance your experience in the Platform;
- Create statistical information and learn about the preferences of users and general trends on the Platform (e.g. understand which features are more popular than others);
- Assist us in keep the Platform safe and secure, and prevent fraud;
- Improve, develop, upgrade the Platform and our Services; and
- Ensure that content on the Platform is presented in an optimal way for you and for your device (e.g. tablet, mobile phone, etc.).
- Provide you with the Services;
- Provide summaries and trending back to users (adherence overtime exercise overtime, etc.);
- Enable the operation of the Platform and administer your Account;
- Request prior authorizations from Partners on your behalf, following up with Partners on such requests, and updating you on status (which may be facilitated by third party service providers we engage from time to time);
- Feed our webscraping algorithm that curates information applicable to you;

- Connect you with various sources, such as pharmaceutical manufacturers, support groups, etc.;
- Create aggregated patient profile reports for internal use and for our pharmaceutical sponsors;
- Create de-identified user-level reports for internal use and for use by our pharmaceutical sponsors;
- Respond to your inquiry;
- Provide the full functionality of the Platform with the main purpose of providing you with tailored, personalized and relevant information, services and resources related to a medical condition, and/or a particular treatment;
- Allow you to interact with Partners within the Platform;
- Contact you by email or via the Platform with proposals and tailored information regarding new products, offers, services, features, enhancements, upgrade opportunities, Clinical Trial opportunities, etc.;
- Contact you by email or via the Platform with proposals and tailored information regarding your input health information, integrated fitness information, and input dietary information;
- Report out metrics and insights to current and/or potential Partners;
- Respond to your technical support requests or other questions concerning the Platform;
- Send notifications (whether general or User-specific) to your device;
- Allow you to set reminders within the Platform;
- Verify your identity when you sign in to the Account in the Platform, as well as verifying your identity for the purpose of dealing with inappropriate interactions and/or fraudulent use of our Platform;
- Determine general geo-location information (i.e., state) from which your device is connected to the Internet and GPS information of your device in order for us to show you geographically relevant content.
- Add your contact details to our mailing list for the purposes of sending you information, status updates relevant to your treatment (when applicable), updates about our developments of our products and services, new offerings, research or news by email, SMS, phone, or through web-browser notification. You have the right to opt-out of these status messages at any time by following the instructions in any such message or by contacting us at: support@redi.health;
- Enable us to contact you for the purpose of providing you with technical assistance and in order to provide the Services;
- Provide you with updates, notices, announcements, and additional information related to us, including with respect to changes made to our Platform's Terms of Service and Privacy Notice;
- Conduct internal operations, including troubleshooting, data analysis, testing, research and statistical purposes;
- Assist us in keeping the Platform safe and secure and for prevention of fraud and crime;
- As part of any merger, acquisition, debt financing, sale of company assets, or other business transaction;

- As part of aggregated, anonymous information to our advertisers, business partners, and other third parties that includes or is based on information about you. We take technical and organizational measures to anonymize your information and to combine it with other users' information, so that it does not directly identify you.
- Comply with our legal obligations and in order to be able to protect our rights and legitimate interests;
- Maintain our data processing records and general administrative purposes; and
- Email tracking- we may use tracking technology within the email we may send you in order to improve interactions with you and to better understand whether our emails were opened and read, and such tracking may include capturing the time and date in which you opened our email messages and the type of device you use to open such emails.

As it pertains to your Sensitive Information, we only use Sensitive Information as follows:

- Your Sensitive Information may be used or disclosed to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with a third party. This also includes providing Sensitive Information to Partners pursuant to our agreements with them to provide services to you regarding your care and treatment.
- To support the operation of Partners.
- Your Sensitive Information will be used, as needed, to obtain payment for health care services provided by integrated Partners that offer features requiring payment.
- Your Sensitive Information may be used or disclosed, as needed, to support the business activities of us or the Partners. These activities include, but are not limited to, consent capture, communications, surveys, quality assessment activities, employee review activities, and conducting or arranging for other business activities.
- With your consent.
- As required by law.

How We Share Your Personal Data?

We respect your privacy and neither disclose your personal information to third parties for money or other valuable consideration (other than as part of a contract where they provide a service to us) nor sell your information for money or other valuable consideration. Moreover, we do not share your personal information with third parties for targeted or cross-context behavioral advertising or in an identifiable way.

If you used one of our Partners to register or currently use their products or services, then we share such data with them.

In addition to using the Personal Data collected by us for the purposes described above, we may also share your Personal Data in the following cases:

a. Our Personnel: Personal Data that we collect and process may be transferred to or accessed by our personnel for the sole purpose of enabling the operation of the Platform and to contact you, as detailed above. Please note that all our personnel that have access to your Personal Data are under an obligation of strict confidentiality with respect to such Personal Data.

b. Service Providers: We share Personal Data with our service providers, including our subsidiary company(ies), commercial software providers, consultants, and data processors who perform services on our behalf, including without limitation, companies that provide analysis, messaging services, and secure data storage.

c. Medical Providers and Other Partners: The Platform serves, among other things, as a platform that eases your communications with the applicable Partners. If you are referred to us by one or more Partners, your Personal Data may be shared with such Partners. We only share your Internet and electronic network activity information to the extent it relates to a demonstrable continuity of care associated to such Partners.

In addition, we may share Personal Data in the following cases: (a) to satisfy any applicable legitimate and binding law, regulation, legal process, subpoena or governmental request; (b) to enforce this Privacy Notice or any other agreement or terms of service between you and ourselves, and to defend against any claims or demands asserted against us by you or on your behalf; (c) to detect, prevent, or otherwise address fraud, security or technical issues; (d) to protect rights, property, or personal safety, of ourselves, our Users or the general public; (e) when we are undergoing any change in control, including by means of merger, acquisition or purchase of all or substantially all of our assets (while such acquired company or investor may be located in countries outside of your jurisdiction); and (f) pursuant to your explicit approval prior to the disclosure.

With the exception of the Sensitive Information we collect to the Health Tracker, discussed in more detail in the “How the Health Tracker Treats User Sensitive Information” section below, the Sensitive Information we collect will only be used and/or disclosed for the following purposes:

- b. Your Sensitive Information may be used or disclosed, as needed, in the following situations:
- (i) Emergency treatment.
 - (ii) We may disclose your Sensitive Information for law enforcement purposes and as required by state or federal law.
 - (iii) To comply with an order in a legal or administrative proceeding, or in response to a subpoena discovery request or other lawful process, but only if efforts have been made, by us or the requesting party, to contact you about the request or to obtain an order from a court or administrative body to protect the requested Sensitive Information.
 - (iv) If it is necessary to avoid a serious threat to the health and safety of you or the public.

- (v) To public health or other authorities charged with preventing or controlling disease, injury or disability, or charged with collecting public health data.
- (vi) To a health oversight agency, such as Health and Human Service (HHS) for activities authorized by law. These activities include audits; civil, administrative or criminal investigations or proceedings; inspections; licensure or disciplinary actions; or other activities necessary for oversight of the health care system, government programs and compliance with civil rights laws.
- (vii) To comply with laws relating to workers' compensation or other similar programs.
- (viii) If you are active military or a veteran, we may disclose your Sensitive Information as required by military command authorities. We may also be required to disclose Sensitive Information to authorized federal officials for the conduct of intelligence or other national security activities.
- (ix) To coroners, or medical examiners for the purposes of identifying a deceased person or determining the cause of death, and to funeral directors as necessary to carry out their duties.
- (x) As otherwise authorized by you.
- (xi) Upon your consent into a Partner's service.
- (xii) To comply with any applicable laws.

We do not process your Sensitive Information to infer characteristics about you, such as to provide them to a search engine of medical conditions.

No Sale/Sharing of Minors' Personal Information; No Targeted Ads to Minors

We do not sell or "share" (for cross-context behavioral advertising) the personal information of minors. We do not use minor profiles for targeting advertising. Where required by law, any sale or sharing of personal information to consumers under 16 would require prior opt-in authorization from the minor (13-15) or the minor's parent/guardian (under 13).

How the Health Tracker Treats Your Sensitive Information

The Health Tracker provides Users a function to track specific symptoms or disease state, including when the attack occurred, the severity of the attack, actions the User took in response to the attack, etc. The Health Tracker also allows you to take a photo of the affected area of your body, upload that photo to the Health Tracker, and share that photo directly with the healthcare provider of your choosing.

Information entered in the Health Tracker attack log is considered private and will not be shared with our partners. Notably, any photo taken and uploaded to the Health Tracker by you will not be shared through the Platform with any person or entity other than the person or entity that you choose to share the photo. Photos sent to a provider via the Platform are transmitted and deleted after delivery or failed delivery attempt.

Uploading exploitative images of minors is illegal. We may block, preserve, and report suspected child sexual abuse material to NCMEC and law enforcement as required by 18 U.S.C. § 2258A.

The photos may contain photos of a User's private areas. As such, you are cautioned to ensure the person or entity you choose with whom to share photos via the Platform is the correct person or entity. Prior to taking a picture and sending it, please confirm the correct recipient email/phone number.

We are not responsible for any sharing of photos via the Health Tracker as Redi.Health merely acts as a conduit between you and with whomever you choose to share the photos.

As such, you should ensure you have reviewed the relevant privacy notices and HIPAA disclosure and authorization forms of those persons or entities with whom you choose to share photos to ensure those policies align with how you would like your photos handled, processed and disclosed.

U.S. State Privacy Rights

This section provides additional disclosures to California, Colorado, Connecticut, Montana, Nevada, Oregon, Texas, Utah, Virginia and Washington residents under their respective state privacy laws, including further information on their rights under such laws.

In this section, when we use the term "personal information" we mean it (or similar term, such as "personal data") as it is defined under those laws.

Verification. We'll need enough detail to understand and respond to your request. We may need to verify your identity to process your requests and may also need to confirm your state residency. To verify your identity, we may require a combination of government identification, or other information. We may also require you to login from a verified valid device or verify that the device you're logging in from is valid.

Authorized Agents. You can have an authorized agent make a request on your behalf, but we'll need to verify your agent's identity. We would also need a copy of a valid power of attorney, or a written and signed permission to exercise your privacy rights on your behalf. We may still need to verify your identity and may ask you to directly confirm that you provided your authorized agent permission to submit the request on your behalf.

Sensitive Information. We process "sensitive personal information" (or similar term, such as "sensitive data") only as reasonably expected for providing the Services that you've requested or as otherwise permitted **without** requiring a corresponding right to restrict or limit such use.

Profiling. We do not undertake any “profiling in furtherance of decisions that produce legal or similarly significant effects” on our creators.

Medical Information. For purposes of California residents, we process “Medical Information” which is “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment” as that term is defined by the California Medical Information Act (“CMIA”).

Consumer Health Data Privacy Notice: If you are Washington or Nevada residents, see our Consumer Health Data Privacy Notice, which explains how we collect share “consumer health data” and how to exercise your rights and choices. We do not geofence around health-care facilities to collect Consumer Health Data or target messages. Washington and Nevada prohibit this use.

Retention. The duration of how long we retain personal information is generally based on how long we need it for the purposes for which it was collected, which includes complying with our legal obligations.

Your Privacy Choices

You may have certain data subject rights:

- **Request to Access:** You have the right to receive a copy of specific pieces of personal data that we have collected about you.
- **Request to Know:** You have a right to receive a description of the categories of personal data collected about you, categories of sources from which we received it, categories of your personal data that we sold or disclosed for a business purpose, categories of third-parties to whom personal data was sold or disclosed for a business purpose, and the purposes for which we collected personal data about you.
- **Request to Delete:** You have the right to request that we delete personal data that we collected from you.
- **Request to Correct:** If you believe we have inaccurate personal data about you, you have the right to ask us to correct it. Please note that we may require that you provide us with the specific data you want us to correct along with all relevant documentation available at the time of your request supporting your belief that the data we have is inaccurate.
- **Request to Opt-out of Sale/Sharing Personal Data:** You have the right to opt-out if you do not wish to receive cross-context behavioral advertising. Please note, that we do not sell or share (as defined by U.S. privacy law) your personal data.
- **Request to Opt-out of Automated Decision-Making/Profiling:** You have the right to opt-out of profiling where the profiling is used in furtherance of decisions that produce legal or similarly significant effects.
- **Right to Limit the Use of Sensitive Personal Information**

If you are a resident of CA, CO, CT, MT, NV, OR, TX, UT, VA or WA, or were in the last 12 months, you may exercise any of the above listed data subject rights, except the Right to Limit the Use of Sensitive Personal Information (see below for instructions on how to exercise that right) by clicking on this Data Subject Rights Form or by emailing us at support@redi.health subject

“Data Subject Rights Request” with you name, contact information, relationship to Redi.Health, and description of the data subject right(s) you wish to exercise.

Appeals. If you are a Colorado, Connecticut, Montana, Oregon, Texas, or Virginia resident, you may appeal our refusal to take action on a request exercising one of your rights mentioned above by contacting us via the information contained in the Contact Us section.

Limit the Use of My Sensitive Personal Information

U.S. State Consumer Data Privacy Laws give some consumers the ability to limit the use and disclosure of their Sensitive Personal Information to only that which is essential for us to provide our services to you. Redi.Health Inc. does not collect Sensitive Information for general marketing purposes and we do not sell or share Sensitive Information as those terms are defined under U.S. State Consumer Data Privacy Laws. You may limit our use of your sensitive personal information by completing this Form.

We will respond to your request to limit as soon as feasible, but no later than 15 business days after receiving a verifiable request.

California Residents

Shine the Light Law: Pursuant to Section 1798.83-.84 of the California Civil Code, residents of California have the right to request from a business, with whom the California resident has an established business relationship, what types of personal information, if any, the business shares with third parties for direct marketing purposes by such third party and the identities of the third parties with whom the business has shared such information in the immediately preceding calendar year. To access this information, please contact us by emailing support@Redi.Health with “CA Shine the Light Privacy Requests” in the subject line. Please note that, under the law, we are not required to respond to your request more than once in a calendar year, nor are we required to respond to any requests that are not sent to the above-designated email.

Medical Information Under CMIA: California residents shall be given access to inspect or get copies of their medical records upon payment of reasonable clerical costs and certain other conditions.

We may disclose you Medical Information as allowed by law without your written authorization, including, when compelled as follows: (1) court order; (2) by board, commission or administrative agency for purposes of adjudication; (3) by a party to a legal action before a court, arbitration, or administrative agency, by subpoena or discovery request; (4) by a board, commission or administrative agency pursuant to an investigative subpoena; (5) by an arbitrator or arbitration panel, when arbitration is lawfully requested by either party; (6) by lawful search warrant; (7) at the “request” of the coroner; or (8) as otherwise specified by law. Except for the circumstances identified above, we will only disclose your Medical Information upon your consent.

Do Not Track

As discussed above, some information about you we obtain automatically through technological means and we may tie this information to Personal Data about you that you provide to us or that we collect from other sources. “Do Not Track Signals” is a browser setting that allows you to signal that you do not want to be tracked online. There is no industry-standard interpretation of Do Not Track signals at this time, and we do not currently respond to Do Not Track signals. Where required by applicable law, however, we recognize Global Privacy Control (“GPC”) signals sent by your browser as a request to opt out of any “sale” or “sharing” of your personal information for purposes of cross-content behavioral advertising. Because we do not sell or share personal information for those purposes, GPC signals will not change the way we process your information in the ordinary course, but they will be honored as a confirming opt-out preference.

Social Media

You should review your privacy settings and options directly with each of the social media platforms and networks that you access to determine your options and choices about sharing information from these sites with us.

Email Communications

You may opt out or otherwise unsubscribe of receiving marketing or other communications from us at any time by following the opt-out / unsubscribe link or other unsubscribe instructions provided in any email message received, or by contacting us using the contact information provided below. If you wish to opt out by sending us an email to the address provided below, please include “Opt-Out” in the email’s subject line and include your name and the email address you used to sign up for communications in the body of the email. Note that, even if you opt out of receiving marketing communications from us, we will still send you order confirmations and other non-marketing related messages.

Push Notifications

You may manage your push notifications, including instructing us not to send you any or specifying the type of push notifications you wish to receive, i.e., sound, banner, lock screen, etc., by changing the notification settings within the Platform or in your device settings. To change via your device settings, go to Settings, to the Platform, and choose your desired notifications from there. If you sent reminders within the Platform, but do not accept push notifications allowing this type of functionality, we will default to emailing you reminder notifications.

Mobile Messaging

For specific terms regarding mobile text/SMS messages (“Mobile Messages”), please see our separate Mobile Messages Terms and Privacy Provisions (the “Mobile Policy”). The terms of the Mobile Policy are incorporated into this Privacy Notice and also apply to your use of the Platform and our Services.

Location of Your Data

Please note that we collect, hold and manage your Personal Data through a third party's cloud-based services, as reasonable for business purposes, which may be located in countries outside of your jurisdiction.

The Personal Data collected from you, as detailed in this Privacy Notice, may be transferred to, and stored at, servers that may be located in countries outside of your jurisdiction and in a country that is not considered to offer an adequate level of protection under your local laws. It may also be processed by us and our suppliers, service providers or partners' staff operating outside your country.

As described in the "Eligibility" section above, the Platform is intended for uses in the United States, including Puerto Rico, and we generally store and process Personal Data in the United States. To the extent any Personal Data is transferred to or processed in another jurisdiction by us or our service providers, we maintain appropriate contractual safeguards designed to ensure an adequate level of protection consistent with applicable law. Where applicable, transfers from the European Economic Area, the United Kingdom, or Switzerland are made in reliance on lawful transfer mechanisms (such as EU-US Data Privacy Framework, the UK Extension to the Data Privacy Framework, the Swiss-US Data Privacy Framework, or the European Commission's Standard Contractual Clauses, as applicable).

We will ensure the confidentiality, integrity and availability of your Personal Data by transferring your Personal Data only to (i) countries approved by the European Commission as having adequate data protection laws; (ii) entities that executed standard contracts that have been approved by the European Commission and which provide an adequate level of high-quality protection, with the recipients of your Personal Data; and (iii) transferring your Personal Data to organizations that are Privacy Shield Scheme certified, as approved by the European Commission.

By submitting your Personal Data through the Platform, you acknowledge, and agree, in jurisdiction where such consent is required, to such transfer, storing and/or processing of Personal Data.

Children's Privacy

As described in the "Eligibility" section above, Accounts on the Platform are held only by adults at least eighteen (18) years old. The Platform is not directed to children under the age of thirteen (13). We rely on age representations made at registration and on the Caregiver-mediated structure of the Platform to keep children from registering on their own. Personal Data concerning a Dependent who is a minor enters the Platform through the Dependent's Caregiver, who is the verifiable consenting party for purposes of the Children's Online Privacy Protection Act (COPPA). The Caregiver may exercise rights with respect to the Dependent's information (including review, deletion, and refusal of further collection) through the means described in this Privacy Notice and in our Terms of Service. If we learn that a child under the age of thirteen (13) has provided Personal Data directly to us without verifiable Caregiver consent, we will delete that data promptly.

Third-Party Service Providers and Third-Party Software

While using the Platform we may be using third-party service providers, who may collect, store and/or process your Personal Data, as detailed in this Privacy Notice.

Note that we collect, hold and/or manage your Personal Data through our authorized third parties whom are vendors of certain products or services (such as hosting cloud services) (including, as applicable, their affiliates) solely and limited to providing us with such requested services, and not for any other purposes.

Third Party Portions and Links

This Privacy Notice only applies to information collected by the Platform. The Platform may contain certain links referring you to third party sites and services. Most of such linked sites and services provide legal documents, including terms of use and privacy policies governing the use thereof, we recommend examining these documents carefully. When you click on links that take you to external websites, you will be subject to the terms and policies of those sites and not ours.

As further detailed in the Terms, the Platform is organized into two areas: (i) the areas managed solely by the Company and not sponsored by any Partner (“Core”); and (ii) the areas made available, sponsored, or supported by one or more Partners (i.e., the Company’s customers, such as hubs, manufacturers, and other partner organizations) (“Connect”).

Each Connect area may be subject to the Terms and Privacy Notice of the applicable Partner if the applicable Partner has requested separate Terms and/or Privacy Notice , while in certain cases Personal Data collected from your usage and activities within the Connect area may be available also to the applicable Partner that wishes to learn, adapt and respond to your individual health needs, medical circumstances, and communication preferences.

In order to enter a Connect area, you may be required to approve the Terms and Privacy Notice applicable to the Connect area. It is always advisable to read such terms carefully before approving them and entering the Connect area in order to know what kind of data about you is being collected.

How We Secure Personal Data?

We take appropriate measures to maintain the security and integrity of our Platform and prevent unauthorized access to it or use thereof through generally accepted industry standard technologies and internal procedures. Specifically, the Platform has been certified HIPAA compliant by our HIPAA compliance vendor and is SOC 2 compliant.

Your Personal Data is hosted on our servers, a backup copy of such information is stored in an encrypted manner on the Amazon Web Services (AWS) servers, and both servers provide advanced strict security standards (both physical and logical).

Some of the security measures that we employ include, without limitation: highly secure services design and implementation using state of the art encryption mechanisms and architecture, restriction of access to your Personal Data to individuals who need access to it in order to process

it on our behalf and implementation of a secured permission management and auditing system, using industry standard firewall and network access filtering as well as security group mechanisms.

Please note, however, that there are inherent risks in transmission of information over the Internet or other methods of electronic storage and we cannot guarantee that unauthorized access or use will never occur.

We will comply with applicable law in the event of any breach of the security, confidentiality, or integrity of your Personal Data and will inform you of such breach if required by applicable law. To the extent that we implement the required security measures under applicable law, we shall not be responsible or liable for unauthorized access, hacking, or other security intrusions or failure to store or the theft, deletion, corruption, destruction, damage, or loss of any data or information included in the Personal Data.

How Long Do We Retain Personal Data?

We will retain the Personal Data for as long as we believe that it is accurate and can be relied upon. Personal Data that is no longer required for the purpose for which it was initially collected will be deleted unless we have a valid justification to retain it that is permitted under applicable law, such as to resolve disputes or comply with our legal obligations. With respect to Medical Information, we dispose of such data in a manner that preserves the information's confidentiality. Any electronic medical record system that stores Medical Information shall reasonably protect and preserve the integrity of electronic Medical Information, and "automatically record and preserve any change or deletion of any electronically stored medical information." The record of any change or deletion will include the identity of the person who accessed and changed the information, the date and time the information was accessed, and the change that was made.

Complaints and Arbitration Agreement

If you feel or believe that your Personal Data rights were harmed in any way or form, you may contact our data protection officer at support@Redi.Health and lodge a complaint. Such complaints shall include how and why you believe your Personal Data rights were harmed, and the required evidence. Our privacy officer will respond to most complaints within 14 days, and shall offer the required remedies.

In the event we are unable to come to a timely mutual resolution of the matter, we remain committed to resolving all disputes in a fair, effective and cost-efficient manner, this Privacy Notice requires that disputes may be resolved in binding arbitration or small claims court. Our arbitration agreement for U.S. disputes, which is set forth below, has been designed to make arbitration as convenient and inexpensive for our customers as possible. We will abide by the terms of our current arbitration provision in all instances. This Privacy Notice and our Terms of Service are governed by Ohio law regardless of where users access or use the Platform.

Arbitration Agreement: United States Only

(a) We and you agree to arbitrate all disputes and claims between us before a single arbitrator. The types of disputes and claims we agree to arbitrate are intended to be broadly interpreted and include:

- Claims arising out of or relating to any aspect of the relationship between us, whether based in contract, tort, statute, fraud, misrepresentation or any other legal theory.
- Claims that arose before these or any prior versions of our Privacy Notice and/or Terms (including, but not limited to, claims relating to advertising);
- Claims that are currently the subject of purported class action litigation in which you are not a member of a certified class; and
- Claims that may arise after termination of this Privacy Notice and/or our Terms.

For the purposes of this Arbitration Agreement, references to “we” and “us” include our respective subsidiaries, affiliates, agents, employees, predecessors in interest, successors and assigns, as well as all authorized or unauthorized users or beneficiaries of our Services or devices under this Privacy Notice and/or our Terms or any prior agreements between us.

Notwithstanding the foregoing, either party may bring an individual action in small claims court. This Arbitration Agreement does not preclude your bringing issues to the attention of federal, state or local agencies. Such agencies can, if the law allows, seek relief against us on your behalf. You agree that, by accessing and using the Platform, you and we are each waiving the right to a trial by jury or to participate in a class action. This Privacy Notice and our Terms evidence a transaction or website use in interstate commerce, and thus the Federal Arbitration Act governs the interpretation and enforcement of this provision. This arbitration provision will survive termination of the Privacy Notice and/or Terms.

(b) A party who intends to seek arbitration must first send, by U.S. certified mail, a written Notice of Dispute (“Notice”) to the other party. A Notice to us should be addressed to: Notice of Dispute, RediHealth, 80 East Rich Street, Suite 660, Columbus, Ohio 43215 (“Notice Address”). The Notice must (a) describe the nature and basis of the claim or dispute and (b) set forth the specific relief sought (“Demand”). If you and we do not reach an agreement to resolve the claim within 30 days after the Notice is received by us, you or we may commence an arbitration proceeding.

During the arbitration, the amount of any settlement offer made by us or you prior to selection of an arbitrator shall not be disclosed to the arbitrator until after the arbitrator determines the amount, if any, to which you or we are entitled.

You may download or copy a form to initiate arbitration from the AAA website (<http://adr.org>) under the “Forms” tab.

(c) After we receive a Notice at the Notice Address that you have commenced arbitration, we will promptly reimburse you for your payment of the filing fee, unless your claim is for more than \$75,000. (Currently, the filing fee is \$125 for claims under \$10,000, but this is subject to change by the arbitration provider. If you are unable to pay this fee, we will pay it directly after receiving a written request to do so at the Notice Address.) The arbitration will be governed by the Commercial Dispute Resolution Procedures and the Supplementary Procedures for Consumer Related Disputes (collectively, the “AAA Rules”) of the American Arbitration Association (the “AAA”), as modified by this Privacy Notice, and will be administered by the AAA. The AAA Rules are available online at www.adr.org or by calling the AAA at 1-800-778-7879. The arbitrator shall be bound by this Privacy Notice and the Terms. Unless you and we agree otherwise, any arbitration hearings will take place in the county (or parish) of your contact address. If your claim is for \$10,000 or less, you may choose whether the arbitration will be conducted solely on the basis of documents submitted to the arbitrator, by a telephonic hearing or by an in-person hearing as established by the AAA Rules. If you choose to proceed either in person or by telephone, we may choose to respond only by telephone or submission. If your claim exceeds \$10,000, the AAA Rules will determine whether you have a right to a hearing.

Regardless of the manner in which the arbitration is conducted, the arbitrator shall issue a reasoned written decision sufficient to explain the essential findings of fact and conclusions of law on which the award is based. You and we agree that any awards or findings of fact or conclusions of law made in an arbitration of their dispute or claim are made only for the purposes of that arbitration and may not be used by any other person or entity in any later arbitration of any dispute or claim involving us. You and we agree that in any arbitration of a dispute or claim, neither of us will rely for preclusive effect on any award or finding of fact or conclusion of law made in any other arbitration of any dispute or claim to which we were a party.

Except as otherwise provided for herein, we will pay all AAA filing, administration, and arbitrator fees for any arbitration initiated in accordance with the notice requirements above. If, however, the arbitrator finds that either the substance of your claim or the relief sought in the Demand is frivolous or brought for an improper purpose (as measured by the standards set forth in Federal Rules of Civil Procedure 11(b)), then the payment of all such fees will be governed by the AAA Rules. In such case, you agree to reimburse us for all monies previously disbursed by us that are otherwise your obligation to pay under the AAA Rules. In addition, if you initiate an arbitration in which you seek more than \$75,000 in damages, the payment of these fees will be governed by the AAA rules. An award may be entered against a party who fails to appear at a duly noticed hearing.

(d) The arbitrator may award injunctive relief only in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by that party's individual claim. **YOU AND WE AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN AN INDIVIDUAL CAPACITY AND NOT AS PLAINTIFFS OR CLASS MEMBERS IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING OR IN THE CAPACITY OF A PRIVATE ATTORNEY GENERAL.** The arbitrator shall not have the power to commit errors of law or legal reasoning, and the parties agree that any injunctive award may be vacated or corrected on appeal by either party to a court of competent jurisdiction for any such error. Each party will bear its own costs and fees on any such appeal. Further, unless both you and we agree otherwise, the arbitrator may not consolidate more than one person's claims or otherwise

preside over any form of a representative or class proceeding. If this specific provision is found to be unenforceable, then the entirety of this arbitration provision shall be null and void.

(e) All aspects of the arbitration proceeding, and any ruling, decision or award by the arbitrator, will be strictly confidential, other than as part of an appeal to a court of competent jurisdiction.

Updates to the Privacy Notice

We reserve the right to amend this Privacy Notice at any time. As our Platform continues to develop, we may add new services and features to our Platform. In the event that these additions affect our Privacy Notice, this Privacy Notice will be updated appropriately. If we make any substantial changes, we will prominently post a notice on the main page and other pages to alert you of the change.

Contact Information

If you have any questions (or comments) concerning this Privacy Notice, please send us an email to the following address: support@Redi.Health or mail to 80 East Rich St, Suite 660, Columbus, Ohio 43215 and we will make every effort to reply within a reasonable timeframe.