

## Prosocial Applications, Inc., Privacy Policy

**Last Updated: January 26, 2024**

RedKangaroo and RK360 are trade names of Prosocial Applications, Inc. and its subsidiaries including Smart Health Records, Inc. (“**Prosocial**,” “**we**,” “**us**” or “**our**”). Prosocial owns and operates websites located at rk360.health, redkangaroo.us, and smartphr.com and all associated, redirected, and linked sites (together, the “**Site**”); digital health privacy, health information exchange, and telehealth cloud software platforms (together, the “**Platform**”); application programming interfaces (**APIs**), databases, hardware devices, mobile device applications or mobile apps, user interfaces, web applications or web portals, and related services (together, the “**Services**”); and electronic health records (the “**Records**”). This Privacy Policy (“**Privacy Policy**”) applies to individuals and enterprises that visit the Site (together, “**Visitors**”), to individuals and enterprises that subscribe to Services and Records (together, “**Subscribers**”), and to individuals and enterprises authorized to access and utilize Services and Records (together, “**Users**”) with individually assigned access and utilization permissions (“**Permissions**”). Refer to Section 1 of our Terms of Service for definitions of these and other terms in this Privacy Policy.

This Privacy Policy applies to information processed through our Site, Platform, Services and Records. You must accept this Privacy Policy to access Site, Services or Records as a Visitor, Subscriber or User. You must also accept the California Privacy Notice in Appendix 1, if you are a California resident.

PLEASE READ THE FOLLOWING PRIVACY POLICY TO UNDERSTAND HOW WE COLLECT, USE, AND SHARE PERSONAL DATA OF VISITORS, SUBSCRIBERS AND USERS OF OUR SITE, PLATFORM, SERVICES AND RECORDS AS WELL AS YOUR CHOICES AND RIGHTS WITH RESPECT TO THIS INFORMATION, AS IT CONSTITUTES A BINDING LEGAL AGREEMENT BETWEEN YOU AND PROSOCIAL. BY ACCESSING OR BROWSING THE SITE OR OTHERWISE ACCESSING OR USING THE SITE, PLATFORM, SERVICES, AND RECORDS YOU HEREBY ACKNOWLEDGE THAT YOU (A) HAVE READ, (B) UNDERSTAND, AND (C) AGREE TO BE BOUND BY OUR TERMS OF SERVICE AND BY THIS PRIVACY POLICY WITHOUT MODIFICATION. IF YOU DO NOT AGREE TO THIS PRIVACY POLICY, THEN YOU MAY NOT VISIT, SUBSCRIBE TO OR USE THE SITE, PLATFORM, SERVICES OR RECORDS.

IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THIS PRIVACY POLICY AND OUR TERMS OF SERVICE, OUR TERMS OF SERVICE SHALL PREVAIL. REFER TO SECTIONS OF OUR TERMS OF SERVICE THAT PREVAIL OVER THIS PRIVACY POLICY, INCLUDING BUT NOT LIMITED TO DEFINITIONS (TERMS AND SERVICES SECTION 1), USER REPRESENTATIONS, RIGHTS AND RESPONSIBILITIES (TERMS AND SERVICES SECTION 3), DATA PROTECTION (TERMS AND SERVICES SECTION 4), DATA RETENTION (TERMS AND SERVICES SECTION 5), TERMINATION OR CANCELLATION OF SERVICES (TERMS AND SERVICES SECTION 6).

Prosocial reserves the right to change or modify the Terms of Service, this Privacy Policy, or any policy, procedure, or guideline of the Site, Platform, Services, Records, or Subscriptions (collectively “**Changes**”) at any time. If, when you became a Subscriber or a User, you supplied us with your email address, we will notify you at that email address of any material Changes, which will be effective immediately upon implementation of Changes and upon active notification of Subscribers

and Users. It is your responsibility to correct and/or update the email address in our files, to assure your timely receipt of notifications about Changes and other matters. Your continued use of the Site, Platform, Services, Records or Subscriptions following the posting or implementation of Changes will confirm your acceptance of such Changes. If the Changes are not acceptable to you, your only option is to stop using the Site, Platform, Services, Records; cancel Subscriptions; export data from Records to storage devices you control; authorize deletion of Records; and uninstall associated mobile and web apps from your devices and computers.

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

## 1. THIRD PARTIES

This Policy does not apply to information processed by third parties, for example, information created and stored by health care providers (“**Providers**”), unless and until we receive your information from them. Please review these third parties’ privacy policies to learn more about how they process your Personal Data.

## 2. HOW WE PROCESS PERSONAL DATA

### 2.1 Personal Data We Process

2.1.1 We may collect and process information that relates to identified or identifiable individuals (“**Personal Data**”). Note that certain Personal Data may include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health information, or information relating to sex life or sexual orientation (“**Special Category Data**”). We collect and process the following categories of Personal Data. Note, specific Personal Data elements listed in each category are only examples and may change.

**Identity Data:** Personal Data used to identify a person, such as your name, photo/avatar, username, identification documents, and other Personal Data you may provide during account registration or to prove your identity.

**Contact Data:** Personal Data used to contact an individual, e.g. email address(es), physical address(es), phone number(s), or usernames/handles, as well as a name or other salutation.

**Financial Data:** Personal Data relating to financial accounts or services, e.g. a credit card or other financial account number, or other relevant information you provide in connection with a financial transaction.

**Insurance Data:** Personal Data relating to your health insurance policy and coverage, including your insurance number. This information may be considered Special Category Data.

**Device Data:** Pseudonymous Personal Data relating to your device, browser, or application e.g. IP addresses, MAC addresses, application ID, cookie identifiers, session

navigation history and similar browsing metadata, and other data generated through applications, browsers, cookies, and similar technologies.

**Health Records:** Health care records, and any Personal Data in them, that we receive from health care Providers, such as allergy records, vital statistics, lab tests and results, prescription/medication data, and information relating to medical procedures and medical conditions. This information includes Special Category Data.

**Health Profile Data:** Personal Data you provide to us about you and your health including, blood type, race, ethnicity, religious affiliation, language, education, diet/digestion, lifestyle, known health conditions and certain medical history, allergies, and medications, and other information relating to your health. This information includes Special Category Data.

**User Content:** Information that a User provides in a message, free text field, video/chat, in a file upload, scan or photo, or unstructured format, including any Personal Data or Special Category Data to the extent contained in or revealed by such content.

## 2.2 Processing of Personal Data

Prosocial processes and uses Personal Data for the following purposes:

### 2.2.1 Registration

**Data:** When you first register an RK360 Record as a Record Owner or Record Administrator or first access an RK360 Record as a User, we will request and process Identity Data, Device Data, and certain Contact Data, such as a copy of driver's license, passport or other ID, and email address. We may also process certain Financial Data or Insurance Data if you choose to subscribe to our Services, or otherwise pay or seek payment for our subscription fees. This Financial Data may be processed by us, a service provider on our behalf, or may be completed outside of our Services (e.g. through the Apple and Google Play App Stores).

**Uses:** We use the Identity Data and Contact Data as necessary to authenticate Users and to provide you with important information about your RK360 Record. Financial Data provided at registration will be used only as necessary to process transactions at your request, or to store your information for use in future payments. Subject to "Your Rights & Choices" (Section 5), we may also use Identity Data and Contact Data in connection with processing of personal data on our Site.

### 2.2.2 Contact Us

**Data:** Our Services may process Identity Data, Contact Data, and User Content when you contact us through the Site.

**Uses:** Subject to Your Rights & Choices (Section 5), our Services will process any Personal Data we collect from our "Contact Us" form to respond to your request, provide you with relevant information, or if appropriate, in connection with Product and Service

## Improvement and Information Security.

### 2.2.3 RK360 Records

**Data:** Our Services allow Users, consistent with their Permissions, to request import of Health Records and other health information into RK360 Records from diverse external sources including the electronic health records of healthcare Providers. In connection with such requests, our Services will process any designated Identity Data, Health Profile Data, Health Records, Insurance Data, and User Content.

Please note: Our Services enable Users, consistent with their Permissions, to request from Providers via intermediary technology services and application programming interfaces (APIs) the import of Health Records, which are generated and controlled by Providers or their business associates. Therefore, data we import into RK360 Records may be inaccurate or incomplete depending upon the content of source records, and the quality of intermediary technology services and APIs. See Your Rights & Choices (Section 5) for information regarding data accuracy and correction.

**Uses:** Our Services generally process Identity Data, Health Profile Data, Health Records, Insurance Data and User Content as necessary to provide our Services, and in accordance with each User's consent, requests, preferences, and Permissions.

Our Services may collect and process Identity Data, which may include driver's license, passport, or insurance information, when you provide patient authorizations and medical power of attorney or upload your insurance information to the Services. This Identity Data is stored by our Services, which offers you tools, consistent with your Permissions and preferences, for you to disclose this information to third parties. This Identity Data is not processed for any purpose other than for operation of our Site and Services, the disclosures you authorize, and subject to Your Rights & Choices (Section 5), in connection with Audit Logs and Information Security.

Subject to Your Rights & Choices (Section 5), and where permitted by law, we may also use Identity Data and Contact Data in connection with processing of personal data on our Site.

### 2.2.4 Get in Touch

**Data:** Our Services allows Users, consistent with their Permissions and subscription status, to contact our customer support agents through a dedicated communication channel. When you contact us, our Services will process Identity Data, Device Data, as well as any User Content you choose to provide.

**Uses:** Subject to Your Rights & Choices (Section 5), our Services will process any Personal Data collected from all communication channels (such as text, chat, email, or phone) in order to respond to your request, provide you with relevant information, or if appropriate, in connection with processing of personal data on our Site.

## 2.2.5 Marketing Communications

**Data:** Our Services may process Identity Data and Contact Data in connection with email and social media marketing communications if you register for our Services, choose to receive marketing communications, or interact with our marketing communications.

**Uses:** Our Services process Identity Data and Contact Data as necessary to provide marketing communications you request. Consistent with our legitimate business interests, we may send you certain marketing and promotional communications if you sign up for those communications or register for our Services. See Your Rights & Choices (Section 5) for information about how you can limit or opt out of this processing.

## 2.2.6 Cookies and Similar Tracking Technologies

**Data:** Our Site and Services, and certain third parties (Section 1), may process Identity Data, Contact Data and Device Data when you interact with cookies and similar technologies on our Site. Our Services may receive this data from third parties to the extent allowed by the applicable partner. Note that privacy policies of third parties may apply to these technologies and data collected.

**Uses:** Subject to Your Rights & Choices (Section 5), we use this information as follows:

for “essential” or “functional” purposes, such as to enable various features of the Site including remembering passwords or staying logged in during your session; and

for “analytics” purposes, consistent with our legitimate interests in how the Site is used or performs, how users engage with and navigate through the Site, what sites users visit before visiting our Site, how often they visit our Site, and other similar information.

**Note:** Some of these technologies may be used by us and/or our third-party partners to identify you across platforms, devices, sites, and services.

## 3. INFORMATION ABOUT SPECIFIC PROCESSING OPERATIONS

### 3.1 Audit Logs

In order to help secure our Services, meet our legal obligations, and help track access to and disclosures of your Personal Data, our Services creates logs that record Device Data, and if available, Identity Data when Health Records and other Personal Data are accessed, viewed, disclosed, modified, or deleted. These logs are subject to Your Rights & Choices (Section 5).

### 3.2 Information Security

Subject to Your Rights & Choices (Section 5), we may also process any Personal Data we possess in order to monitor the use of our Services and Site for malicious activity, detect systems vulnerabilities, and as otherwise appropriate to maintain the integrity and security of our Services and Site and the Personal Data we process.

### 3.3 Product and Service Improvement

Subject to Your Rights & Choices (Section 5), we may process any Identity Data, Contact Data, Financial Data, Device Data, and User Content in order to analyze how users interact with our Services or Site, in connection with market research, for product and service improvements, and as necessary to monitor and maintain the integrity and security of our Services, Site and the data we process.

### 3.4 Research and Public Health

We may also process and disclose your Personal Data for uses related to medical research, public health, product recalls and other medical product liability/safety matters, and for other research and public health/safety grounds, to the extent and under the conditions allowed by applicable law.

### 3.5 Additional Processing

If we process Personal Data in connection with our Services or Site in a way not described in this Policy, this Policy will still apply generally (e.g., with respect to Your Rights & Choices (Section 5)), unless otherwise stated when you provide it.

Note that we may, without your consent, also process your Personal Data on certain public interest grounds. For example, we may process information as necessary to fulfill our legal obligations, to protect the vital interests of any individuals, or otherwise in the public interest. Please see Data Sharing (Section 4) for more information about how we disclose Personal Data in extraordinary circumstances.

## 4. DATA SHARING

**As stated in Section 3.4 of the Prosocial Terms of Service, it is the responsibility of Distributors, Record Owners, and Record Administrators to select trusted Users for Record Permissions, grant them suitable permissions, review audit reports, change or remove User permissions as needed, promptly report User misconduct to Prosocial and the appropriate authorities, and take all necessary actions to remedy User misconduct and prevent additional misconduct. The foregoing provision supersedes any HIPAA Business Associates Agreement or Notice of Privacy Practices of distributors and of corporate or government entities even if agreed to by patients or their personal representatives. The foregoing provision determines how we enable data sharing with the following categories of recipients:**

### 4.1 Record Administrators & Other Users

A Record Administrator, whether appointed by the Record Owner or acting as personal representative, guardian, or medical power of attorney for the Record Owner, may have Permissions for access to Personal Data in the RK360 Record of the Record Owner, including Medical Records and Medical Profile Data. Record Administrators may also have Permissions for disclosure of that information to third parties or for granting Permissions for access to other subordinate Users, to the extent such functionality is made available through our Services and the Record Administrator has requisite Permissions.

## 4.2 Providers

Our Services enable the exchange of medical information and other contents of RK360 Records with external sources and recipients of designated information such as Healthcare Providers. When Users, consistent with their Permissions, utilize tools in RK360 Records to exchange Personal Data in RK360 Records through our Services, our Services may share any designated information including Health Record Data, Health Profile Data, and any Sensitive Personal Data.

## 4.3 Treatment, Payment, and Healthcare Operations

To the extent we process Personal Data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we may disclose such Health Record Data and Health Profile Data, Contact Data, Identity Data, and Insurance Data where authorized for Treatment, Payment, and Healthcare Operations. These include activities such as disclosing information to Providers, for our product and service Improvement, or if necessary, to bill patients or insurance providers.

## 4.4 Service Providers

In connection with our general business operations, product/service improvements, to enable certain features, and in connection with our other legitimate business interests, we may share any Personal Data with service providers or subprocessors who provide certain services or process data on our behalf.

## 4.5 Affiliates

Subject to Your Rights & Choice (Section 5), in order to streamline certain business operations and develop products and services that better meet the interests and needs of our Users, and inform our customers about relevant products and services, we may share your Personal Data with any of our current or future affiliated entities, subsidiaries, and parent companies.

## 4.6 Corporate Events

Any Personal Data may be processed without your consent in the event that we go through a business transition, such as a merger, acquisition, liquidation, or sale of all or a portion of our assets. For example, Personal Data may be part of the assets transferred, or may be disclosed (subject to confidentiality restrictions) during the due diligence process for a potential transaction.

## 4.7 Legal Disclosures

In limited circumstances, we may, without notice or your consent, access and disclose your Personal Data, any communications sent or received by you, and any other information that we may have about you to the extent we believe such disclosure is legally required, to prevent or respond to a crime, or for other law enforcement and national security reasons, to investigate violations of our Terms of Service, or when the disclosure is in the vital interests of us or any person. Note, these disclosures may be made to governments or other authorities in jurisdictions that do not ensure the same degree of protection of your Personal Data as your home jurisdiction. We may, in our sole discretion (but without any obligation), object to the disclosure of your Personal Data to such parties on any lawful grounds we may have.

## 4.8 Other Disclosures

We may disclose any Personal Data without your consent on certain public interest grounds. For example, we may process information as necessary to fulfill our legal obligations, for public health and other matters in the public interest, to medical providers or healthcare organizations, medical examiners, in connection with organ and tissue donor requests, or where otherwise allowed by applicable law.

## 5. YOUR RIGHTS & CHOICES

### 5.1 Your Rights

Applicable law may grant you some or all of the following rights in your Personal Data. To the extent applicable law grants you these rights, you may exercise these rights using the methods set forth below, you may read Frequently Asked Questions posted on our website [www.rk360.health](http://www.rk360.health), or you may email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us). Please note: we may require that you provide additional Personal Data to exercise these rights, e.g. Identity Data that is necessary to prove you are authorized with requisite Permissions to make a request.

**5.1.1 Access:** You may access the Personal Data that we process to the extent required and permitted by law. Further, our Services offers you tools, consistent with your permissions as a User, for securely accessing your personal data, including Health Records, Health Profile Data, data from Audit Logs, and other information about your RK360 Record. We will explain how to use these tools but cannot utilize these tools on your behalf.

**5.1.2 Rectification:** Our Services offers you tools, consistent with your permissions as a User, for correcting any Personal Data that our Services hold about you to the extent required and permitted by law. You may be able to make changes to Personal Data, such as Account Registration Data and Medical Profile Data through tools our Services offer. We will explain how to use these tools but cannot utilize these tools on your behalf.

Please note: Our Services store and display copies of Health Records that are maintained in Providers' systems; we do not control and cannot alter the content of Providers' Health Records. Please contact the relevant Provider to exercise your right to correct Health Records in their systems. Updated Health Records will be reflected in our Services when updated by Providers and only if Users, consistent with their Permissions, authorize our Services to receive updated Health Records.

**5.1.3 Erasure:** Our Services offer you tools, consistent with your Permissions as a User, for deletion of Health Records, Health Profile Data, account registration data and other contents of RK360 Records. You may not, however, delete the Audit Logs that document User activities on the Service and in RK360 Records. We will explain how to use these tools but cannot utilize these tools on your behalf.

Please note: we store and display copies of Health Records that are maintained in Providers' systems if they are shared with us; we do not control and cannot delete Health Records stored in Providers' systems. Please contact relevant Providers to exercise your right to delete your primary Health Records from their systems.



5.1.4 Data Portability: To the extent required by applicable law, our Services will enable you to export and send to destination storage locations you control, to Providers or to other third parties, copies of certain contents of your RK360 Record in a common portable format. Before you delete Data, our Services will remind you to export a copy of your Data to a destination storage location you control. To export Data, you may use the data sharing functionality that our Services offer, and you may employ as destinations your email address or the email address of a third party you select. We will explain how to use these tools but cannot utilize these tools on your behalf.

5.1.5 Complaints: You have the right to contact or file a complaint with us, as well as regulators or supervisory authorities, about our processing of Personal Data. To file a complaint with us, email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us). To file a complaint with governmental bodies, please contact your local data protection or consumer protection authority. In the US, you may be able to file a complaint with the Federal Trade Commission, or if appropriate, the Department of Health and Human Services, in each case, by submitting a complaint through their online complaint processes. We will not retaliate against you for filing a complaint.

5.1.6 California Rights: Residents of California (and others to the extent required by applicable law) may request a list of Personal Data we have disclosed about you to Third Parties (Section 1) for direct marketing purposes during the preceding calendar year (if any). Please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

5.1.7 HIPAA: To the extent required by applicable law, we will provide you with an accounting of the disclosures of your Health Data or Health Profile Data (if any). To do so, please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

## 5.2 Your Choices

It is possible for you to use portions of our Site without providing any Personal Data, but you may not be able to access certain features or view certain content. You have the following choices regarding the Personal Data we process, however, please note that we may not be required to agree to a requested restriction to the extent permitted by law:

5.2.1 Data Collection & Sharing: You may generally control how Personal Data is shared with us, and how we share your Personal Data. You can control what Personal Data we collect by modifying Permissions you grant to Providers or by modifying your authorizations to share data with third parties. Additionally, you may change your authorization for our Services to continuously import new contents into your RK360 Record via APIs through tools our Services offer. You may also limit sharing of any Health Records and Health Profile Data, as well as any other Personal Data (including data shared with third parties and subordinate Users) through tools our Services offer.

Please note: Only Account Administrators may control the Permissions of subordinate Users through tools our Services offer. You may contact us through Get in Touch channels (Section 2.2.4) for guidance about how to employ tools our Services offer, but we cannot utilize these tools on your behalf.

5.2.2 Consent: If you consent to any other processing of your Personal Data, you may withdraw your consent at any time.

Please note: Your sole means of revoking consent may be to delete your RK360 Record and the Records you administer for others.

5.2.3 Direct Marketing: “**Direct Marketing**” means messages to you about offerings unrelated to our Services and Subscriptions. You may have a legal right in certain circumstances not to receive Direct Marketing messages, in which case, you will only receive Direct Marketing messages if you consent or opt-in via links in such messages.

Please note: Messages to you about our Services and Subscriptions do not constitute Direct Marketing. Your sole means of revoking consent to such messages may be to delete your RK360 Record and the Records you administer for others.

5.2.4 Cookies & Similar Tech: If you do not want information collected through the use of cookies and similar technologies, you must manage/deny cookies (and certain technologies) using your browser’s settings menu. You must opt out of third-party services directly via the third party.

## 6. SECURITY

We are required by law to maintain the privacy of your Health Records and Health Profile Data, and we implement reasonable and appropriate security measures to safeguard the Personal Data you provide us. However, we sometimes share Personal Data with third parties as noted above, and we do not have control over third parties’ security processes. Further, certain methods of sharing your Health Records you may choose to use may present risks to the confidentiality of Sensitive Personal Data. We do not warrant perfect security and we do not provide any guarantee that your Personal Data or any other information you provide us will remain secure, nor will we be liable for any unauthorized disclosures that occur following your choice to share Personal Data with Users or recipients you designate, such as Providers. We will notify you if there is a breach of the security of unsecured Personal Data we may process, where such notice is required by law.

6.1 No Data Selling: As stated in Section 4.1 of our Terms of Service, we do not sell personally identifiable User Data or RK360 Record Contents including for targeted marketing.

## 7. DATA RETENTION

Our Services keep the Medical Records and Profile Data of Users until those Users employ the tools our Services offer, consistent with their Permissions, to delete that data at which point we retain only Audit Logs of User activity in accordance with Your Rights & Choices (Section 5). Otherwise, our Services retain Personal Data for so long as it, in our discretion, remains relevant to its purpose, and in any event, for so long as is required by law. To the extent our Services retain any Personal Data, we will review retention periods periodically, and may pseudonymize or anonymize data held for longer periods, if appropriate.

Please note: For our prevailing Data Retention policy, see Section 5 of our Terms of Service. Your sole means of revoking consent may be to delete your RK360 Record and the Records you administer for others.

## 8. MINORS

Our Services and Site are neither directed at nor intended for use by minors under the age of majority in the relevant jurisdiction. Further, we do not knowingly collect Personal Data from such individuals unless we receive the consent of the minor's parent or guardian. If we learn that we have inadvertently done so, we will promptly delete it. Do not access or use the Service or Site if you are not of the age of majority in your jurisdiction unless you have the consent of your parent or guardian.

## 9. INTERNATIONAL TRANSFERS

We operate in and use Internet service providers located in the United States. If you are located outside the U.S., your Personal Data may be transferred to the U.S. The U.S. does not provide the same legal protections guaranteed to Personal Data in the European Union. Accordingly, your Personal Data may be transferred to the U.S. pursuant to the EU-U.S. Privacy Shield Framework, the Standard Contractual Clauses, or other adequacy mechanisms, or pursuant to exemptions provided under EU law.

## 10. INFORMATION FOR USERS IN THE EUROPEAN ECONOMIC AREA (EEA)

### 10.1 Controller

Prosocial Applications, Inc. is the data controller for Personal Data collected under this Policy.

### 10.2 Legal bases for processing

The legal bases of our processing of your Personal Data are primarily, but not exclusively, described in the following sections of this Privacy Policy.

- Section 1. THIRD PARTIES
- Section 2. HOW WE PROCESS PERSONAL DATA
- Section 3. INFORMATION ABOUT SPECIFIC PROCESSING OPERATIONS
- Section 4. DATA SHARING
- Section 5. YOUR RIGHTS & CHOICES
- Section 6. SECURITY
- Section 7. DATA RETENTION
- Section 8. MINORS
- Section 9. INTERNATIONAL TRANSFERS

### 10.3 Rights of EU Users

10.3.1 Right to Object: Where we process data on the basis of our legitimate interests, you can object to that processing to extent allowed by law. Note that we must only limit processing where our interests in processing do not override an individual's interests, rights, and freedoms, or the processing is not for the establishment exercise, or defense of a legal claim. Email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) with your objections to data processing.

Please note: Your sole means of objection may be to delete your RK360 Record and the Records you administer for others.

10.3.2 Right to Restrict: You may restrict processing of your Personal Data, for any reason, by using the tools our Services provide to first export contents of your RK360 Record, and of the Records you administer for others, to storage destinations you control, and then to delete those Records. However, we cannot utilize these tools on your behalf.

## 11. UPDATES TO THIS PRIVACY POLICY

As stated above, Prosocial reserves the right to change or modify the Terms of Service, this Privacy Policy, or any policy, procedure, or guideline of the Site, Platform, Services, Records, or Subscriptions (collectively Changes) at any time. If, when you became a Subscriber or a User, you supplied us with your email address, we will notify you at that email address of any material Changes, which will be effective immediately upon implementation of Changes and upon active notification of Subscribers and Users. It is your responsibility to correct and/or update the email address in our files, to assure your timely receipt of notifications about Changes and other matters. Your continued use of the Site, Platform, Services, Records or Subscriptions following the posting or implementation of Changes will confirm your acceptance of such Changes. If the Changes are not acceptable to you, your only option is to stop using the Site, Platform, Services, Records; cancel Subscriptions; export data from Records to storage devices you control; authorize deletion of Records; and uninstall associated mobile and web apps from your devices and computers.

## 12. CONTACT US

By Postal Mail:

Chief Technology Officer

Prosocial Applications, Inc.

1905 15th St. #4585

Boulder CO 80302-4585 USA

By email: [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us)

## Appendix 1. California Privacy Notice

This Privacy Notice for California Residents (this “**California Notice**”) is a supplemental notice that is expressly made part of the Privacy Policy to which it is appended and is solely for California resident consumers.

RedKangaroo and RK360 are trade names of Prosocial Applications, Inc. and its subsidiaries including Smart Health Records, Inc. (“**Prosocial**,” “**we**,” “**us**” or “**our**”). Prosocial owns and operates websites located at rk360.health, redkangaroo.us, and smartphr.com and all associated, redirected, and linked sites (together, the “**Site**”); digital health privacy, health information exchange, and telehealth cloud software platforms (together, the “**Platform**”); application programming interfaces (**APIs**), databases, hardware devices, mobile device applications or mobile apps, user interfaces, web applications or web portals, and related services (together, the “**Services**”); and electronic health records (the “**Records**”). This Privacy Policy (“**Privacy Policy**”) applies to individuals and enterprises that visit the Site (together, “**Visitors**”), to individuals and enterprises that subscribe to Services and Records (together, “**Subscribers**”), and to individuals and enterprises authorized to access and utilize Services and Records (together, “**Users**”) with individually assigned access and utilization permissions (“**Permissions**”). Refer to Section 1 of our Terms of Service for definitions of these and other terms in this Privacy Policy.

This California Notice applies to information processed through our Site, Platform, Services and Records. If you are a California resident, you must accept this California Notice, our Privacy Policy and our Terms of Service to access Site, Services or Records as a Visitor, Subscriber or User.

PLEASE READ THE PRIVACY POLICY AND THE FOLLOWING CALIFORNIA NOTICE TO UNDERSTAND HOW WE COLLECT, USE, AND SHARE PERSONAL DATA OF VISITORS, SUBSCRIBERS AND USERS OF OUR SITE, PLATFORM, SERVICES AND RECORDS AS WELL AS YOUR CHOICES AND RIGHTS WITH RESPECT TO THIS INFORMATION, AS IT CONSTITUTES A BINDING LEGAL AGREEMENT BETWEEN YOU AND PROSOCIAL. BY ACCESSING OR BROWSING THE SITE OR OTHERWISE ACCESSING OR USING THE SITE, PLATFORM, SERVICES, AND RECORDS YOU HEREBY ACKNOWLEDGE THAT YOU (A) HAVE READ, (B) UNDERSTAND, AND (C) AGREE TO BE BOUND BY OUR TERMS OF SERVICE, OUR PRIVACY POLICY, AND THIS CALIFORNIA NOTICE WITHOUT MODIFICATION. IF YOU DO NOT AGREE TO OUR TERMS OF SERVICE, OUR PRIVACY POLICY, AND THIS CALIFORNIA NOTICE, THEN YOU MAY NOT VISIT, SUBSCRIBE TO OR USE THE SITE, PLATFORM, SERVICES OR RECORDS.

IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THIS CALIFORNIA NOTICE AND OUR TERMS OF SERVICE, OUR TERMS OF SERVICE SHALL PREVAIL. REFER TO SECTIONS OF OUR TERMS OF SERVICE THAT PREVAIL OVER THIS PRIVACY POLICY, INCLUDING BUT NOT LIMITED TO DEFINITIONS (TERMS AND SERVICES SECTION 1), USER REPRESENTATIONS, RIGHTS AND RESPONSIBILITIES (TERMS AND SERVICES SECTION 3), DATA PROTECTION (TERMS AND SERVICES SECTION 4), DATA RETENTION (TERMS AND SERVICES SECTION 5), TERMINATION OR CANCELLATION OF SERVICES (TERMS AND SERVICES SECTION 6).

Prosocial reserves the right to change or modify the Terms of Service, the Privacy Policy, this California Notice or any policy, procedure, or guideline of the Site, Platform, Services, Records, or Subscriptions (collectively “**Changes**”) at any time. If, when you became a Subscriber or a User, you supplied us with your email address, we will notify you at that email address of any material Changes, which will be effective immediately upon implementation of Changes and upon active notification of Subscribers and Users. It is your responsibility to correct and/or update the email address in our files, to assure your timely receipt of notifications about Changes and other matters. Your continued use of the Site, Platform, Services, Records or Subscriptions following the posting or implementation of Changes will confirm your acceptance of such Changes. If the Changes are not acceptable to you, your only option is to stop using the Site, Platform, Services, Records; cancel Subscriptions; export data from Records to storage devices you control; authorize deletion of Records; and uninstall associated mobile and web apps from your devices and computers.

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

## 1. THIRD PARTIES

This Policy does not apply to information processed by third parties, for example, information created and stored by health care providers (“**Providers**”), unless and until we receive your information from them. Please review these third parties’ privacy policies to learn more about how they process your Personal Data.

## 2. PERSONAL DATA WE MAY COLLECT

2.1 The California Consumer Privacy Act of 2018 (the “CCPA”) requires certain disclosures to California residents with respect to the types of Personal Data we collect from Users of our Services that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household (“Personal Data”), the sources of such Personal Data, and third parties with whom we may share such information.

2.2 We may collect and process Personal Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health information, or information relating to sex life or sexual orientation (“**Special Category Data**”). We collect and process the following categories of Personal Data. Note that specific Personal Data elements listed in each category are only examples and may change.

**Identity Data:** Personal Data used to identify a person, such as your name, photo/avatar, username, identification documents, and other Personal Data you may provide during account registration or to prove your identity.

**Contact Data:** Personal Data used to contact an individual, e.g. email address(es), physical address(es), phone number(s), or usernames/handles, as well as a name or other salutation.

**Financial Data:** Personal Data relating to financial accounts or services, e.g. a credit card or other financial account number, or other relevant information you provide in connection

with a financial transaction.

**Insurance Data:** Personal Data relating to your health insurance policy and coverage, including your insurance number. This information may be considered Special Category Data.

**Device Data:** Pseudonymous Personal Data relating to your device, browser, or application e.g. IP addresses, MAC addresses, application ID, cookie identifiers, session navigation history and similar browsing metadata, and other data generated through applications, browsers, cookies, and similar technologies.

**Health Records:** Health care records, and any Personal Data in them, that we receive from health care Providers, such as allergy records, vital statistics, lab tests and results, prescription/medication data, and information relating to medical procedures and medical conditions. This information includes Special Category Data.

**Health Profile Data:** Personal Data you provide to us about you and your health including, blood type, race, ethnicity, religious affiliation, language, education, diet/digestion, lifestyle, known health conditions and certain medical history, allergies, and medications, and other information relating to your health. This information includes Special Category Data.

**User Content:** Information that a User provides in a message, free text field, video/chat, in a file upload, scan or photo, or unstructured format, including any Personal Data or Special Category Data to the extent contained in or revealed by such content.

2.3 Personal Data does not include publicly available information from government records, consumer information, information that is excluded from the scope of the CCPA, Personal Data covered by sector-specific privacy laws, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act or California Financial Information Privacy Act, and the Driver's Privacy Protection Act of 1994.

### 3. USES OF PERSONAL DATA

Prosocial processes and uses Personal Data for the following purposes:

#### 3.1 Registration

**Data:** When you first register an RK360 Record as a Record Owner or Record Administrator or first access an RK360 Record as a User, we will request and process Identity Data, Device Data, and certain Contact Data, such as a copy of driver's license, passport or other ID, and email address. We may also process certain Financial Data or Insurance Data if you choose to subscribe to our Services, or otherwise pay or seek payment for our subscription fees. This Financial Data may be processed by us, a service provider on our behalf, or may be completed outside of our Services (e.g. through the Apple and Google Play App Stores).

**Uses:** We use the Identity Data and Contact Data as necessary to authenticate Users and

to provide you with important information about your RK360 Record. Financial Data provided at registration will be used only as necessary to process transactions at your request, or to store your information for use in future payments. Subject to “Your Rights & Choices” (Section 5), we may also use Identity Data and Contact Data in connection with processing of personal data on our Site.

### 3.2 Contact Us

**Data:** Our Services may process Identity Data, Contact Data, and User Content when you contact us through the Site.

**Uses:** Subject to Your Rights & Choices (Section 5), our Services will process any Personal Data we collect from our “Contact Us” form to respond to your request, provide you with relevant information, or if appropriate, in connection with Product and Service Improvement and Information Security (Section 3.3 of the Privacy Policy).

### 3.3 RK360 Records

**Data:** Our Services allow Users, consistent with their Permissions, to request import of Health Records and other health information into RK360 Records from diverse external sources including the electronic health records of health care Providers. In connection with such requests, our Services will process any designated Identity Data, Health Profile Data, Health Records, Insurance Data, and User Content.

Please note: Our Services enable Users, consistent with their Permissions, to request from Providers via intermediary technology services and application programming interfaces (APIs) the import of Health Records, which are generated and controlled by Providers or their business associates. Therefore, data we import into RK360 Records may be inaccurate or incomplete depending upon the content of source records, and the quality of intermediary technology services and APIs. See Your Rights & Choices (Section 5) for information regarding data accuracy and correction.

**Uses:** Our Services generally process Identity Data, Health Profile Data, Health Records, Insurance Data and User Content as necessary to provide the Service, and in accordance with each User’s consent, requests, preferences, and Permissions.

Our Services may collect and process Identity Data, which may include driver’s license, passport, or insurance information, when you provide patient authorizations and medical power of attorney or upload your insurance information to the Service. This Identity Data is stored by our Services, which offers you tools, consistent with your Permissions and preferences, for you to disclose this information to third parties. This Identity Data is not processed for any purpose other than for operation of our Site and Services, the disclosures you authorize, and subject to Your Rights & Choices (Section 5), in connection with Audit Logs (Section 3.1 of the Privacy Policy) and Information Security (Section 3.2 of the Privacy Policy).

Subject to Your Rights & Choices (Section 5), and where permitted by law, we may



also use Identity Data and Contact Data in connection with processing of personal data on our Site.

### 3.4 Get in Touch

**Data:** Our Services allows Users, consistent with their Permissions and subscription status, to contact our customer support agents through a dedicated communication channel. When you contact us, our Services will process Identity Data, Device Data, as well as any User Content you choose to provide.

**Uses:** Subject to Your Rights & Choices (Section 5), our Services will process any Personal Data collected from all communication channels (such as text, chat, email, or phone) in order to respond to your request, provide you with relevant information, or if appropriate, in connection with processing of personal data on our Site.

### 3.5 Marketing Communications

**Data:** Our Services may process Identity Data and Contact Data in connection with email and social media marketing communications if you register for our Services, choose to receive marketing communications, or interact with our marketing communications.

**Uses:** Our Services process Identity Data and Contact Data as necessary to provide marketing communications you request. Consistent with our legitimate business interests, we may send you certain marketing and promotional communications if you sign up for those communications or register for our Services. See Your Rights & Choices (Section 5) for information about how you can limit or opt out of this processing.

### 3.6 Cookies and Similar Tracking Technologies

**Data:** Our Site and Services, and certain third parties (Section 1), may process Identity Data, Contact Data and Device Data when you interact with cookies and similar technologies on our Site. Our Services may receive this data from third parties to the extent allowed by the applicable partner. Note that privacy policies of third parties may apply to these technologies and data collected.

**Uses:** Subject to Your Rights & Choices (Section 5), we use this information as follows:

for “essential” or “functional” purposes, such as to enable various features of the Site including remembering passwords or staying logged in during your session; and

for “analytics” purposes, consistent with our legitimate interests in how the Site is used or performs, how users engage with and navigate through the Site, what sites users visit before visiting our Site, how often they visit our Site, and other similar information.

**Note:** Some of these technologies may be used by us and/or our third-party partners to identify you across platforms, devices, sites, and services.

## 4. DATA SHARING

**As stated in Section 3.4 of the Prosocial Terms of Service, it is the responsibility of Distributors, Record Owners, and Record Administrators to select trusted Users for Record Permissions, grant them suitable Permissions, review audit reports, change or remove User Permissions as needed, promptly report User misconduct to Prosocial and the appropriate authorities, and take all necessary actions to remedy User misconduct and prevent additional misconduct. The foregoing provision supersedes any HIPAA Business Associates Agreement or Notice of Privacy Practices of distributors and of corporate or government entities even if agreed to by patients or their personal representatives. The foregoing provision determines how we enable data sharing with the following categories of recipients:**

### 4.1 Record Administrators & Other Users

A Record Administrator, whether appointed by the Record Owner or acting as personal representative, guardian, or medical power of attorney for the Record Owner, may have Permissions for access to Personal Data in the RK360 Record of the Record Owner, including Medical Records and Medical Profile Data. Record Administrators may also have Permissions for disclosure of that information to third parties or for granting Permissions for access to other subordinate Users, to the extent such functionality is made available through our Services and the Record Administrator has requisite Permissions.

### 4.2 Providers

Our Services enable the exchange of medical information and other contents of RK360 Records with external sources and recipients of designated information such as Healthcare Providers. When Users, consistent with their Permissions, utilize tools in RK360 Records to exchange Personal Data in RK360 Records through our Services, our Services may share any designated information including Health Record Data, Health Profile Data, and any Sensitive Personal Data.

### 4.3 Treatment, Payment, and Healthcare Operations

To the extent we process personal data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we may disclose such Health Record Data and Health Profile Data, Contact Data, Identity Data, and Insurance Data where authorized for Treatment, Payment, and Healthcare Operations. These include activities such as disclosing information to Providers, for our product and service Improvement, or if necessary, to bill patients or insurance providers.

### 4.4 Service Providers

In connection with our general business operations, product/service improvements, to enable certain features, and in connection with our other legitimate business interests, we may share any Personal Data with service providers or subprocessors who provide certain services or process data on our behalf.

### 4.5 Affiliates

Subject to Your Rights & Choices (Section 5), in order to streamline certain business operations and

develop products and services that better meet the interests and needs of our Users, and inform our customers about relevant products and services, we may share your Personal Data with any of our current or future affiliated entities, subsidiaries, and parent companies.

#### 4.6 Corporate Events

Any Personal Data may be processed without your consent in the event that we go through a business transition, such as a merger, acquisition, liquidation, or sale of all or a portion of our assets. For example, Personal Data may be part of the assets transferred, or may be disclosed (subject to confidentiality restrictions) during the due diligence process for a potential transaction.

#### 4.7 Legal Disclosures

In limited circumstances, we may, without notice or your consent, access and disclose your Personal Data, any communications sent or received by you, and any other information that we may have about you to the extent we believe such disclosure is legally required, to prevent or respond to a crime, or for other law enforcement and national security reasons, to investigate violations of our Terms of Service, or when the disclosure is in the vital interests of us or any person. Note, these disclosures may be made to governments or other authorities in jurisdictions that do not ensure the same degree of protection of your Personal Data as your home jurisdiction. We may, in our sole discretion (but without any obligation), object to the disclosure of your Personal Data to such parties on any lawful grounds we may have.

#### 4.8 Other Disclosures

We may disclose any Personal Data without your consent on certain public interest grounds. For example, we may process information as necessary to fulfill our legal obligations, for public health and other matters in the public interest, to medical providers or healthcare organizations, medical examiners, in connection with organ and tissue donor requests, or where otherwise allowed by applicable law.

### 5. YOUR RIGHTS & CHOICES

#### 5.1 Your Rights

Applicable law may grant you some or all of the following rights in your Personal Data. To the extent applicable law grants you these rights, you may exercise these rights using the methods set forth below, you may read Frequently Asked Questions posted on our website [www.rk360.health](http://www.rk360.health), or you may email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us). Please note: we may require that you provide additional Personal Data to exercise these rights, e.g. Identity Data that is necessary to prove you are authorized with requisite Permissions to make a request.

**5.1.1 Access:** You may access the Personal Data that we process to the extent required and permitted by law. Further, our Services offers you tools, consistent with your permissions as a User, for securely accessing your personal data, including Health Records, Health Profile Data, data from Audit Logs, and other information about your RK360 Record. We will explain how to use these tools but cannot utilize these tools on your behalf.

5.1.2 Rectification: Our Services offers you tools, consistent with your permissions as a User, for correcting any Personal Data that our Services hold about you to the extent required and permitted by law. You may be able to make changes to Personal Data, such as Account Registration Data and Medical Profile Data through tools our Services offer. We will explain how to use these tools but cannot utilize these tools on your behalf.

Please note: Our Services store and display copies of Health Records that are maintained in Providers' systems; we do not control and cannot alter the content of Providers' Health Records. Please contact the relevant Provider to exercise your right to correct Health Records in their systems. Updated Health Records will be reflected in our Services when updated by Providers and only if Users, consistent with their Permissions, authorize our Services to receive updated Health Records.

5.1.3 Erasure: Our Services offer you tools, consistent with your Permissions as a User, for deletion of Health Records, Health Profile Data, account registration data and other contents of RK360 Records. You may not, however, delete the Audit Logs that document User activities on the Service and in RK360 Records. We will explain how to use these tools but cannot utilize these tools on your behalf.

Please note: we store and display copies of Health Records that are maintained in Providers' systems if they are shared with us; we do not control and cannot delete Health Records stored in Providers' systems. Please contact relevant Providers to exercise your right to delete your primary Health Records from their systems.

5.1.4 Data Portability: To the extent required by applicable law, our Services will enable you to export and send to destination storage locations you control, to Providers or to other third parties, copies of certain contents of your RK360 Record in a common portable format. Before you delete Data, our Services will remind you to export a copy of your Data to a destination storage location you control. To export Data, you may use the data sharing functionality that our Services offer, and you may employ as destinations your email address or the email address of a third party you select. We will explain how to use these tools but cannot utilize these tools on your behalf.

5.1.5 Complaints: You have the right to contact or file a complaint with us, as well as regulators or supervisory authorities, about our processing of Personal Data. To file a complaint with us, email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us). To file a complaint with governmental bodies, please contact your local data protection or consumer protection authority. In the US, you may be able to file a complaint with the Federal Trade Commission, or if appropriate, the Department of Health and Human Services, in each case, by submitting a complaint through their online complaint processes. We will not retaliate against you for filing a complaint.

5.1.6 California Rights: Residents of California (and others to the extent required by applicable law) may request a list of Personal Data we have disclosed about you to Third Parties (Section 1) for direct marketing purposes during the preceding calendar year (if any). Please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

5.1.7 HIPAA: To the extent required by applicable law, we will provide you with an accounting of the disclosures of your Health Data or Health Profile Data (if any). To do so, please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

## 5.2 Your Choices

It is possible for you to use portions of our Site without providing any Personal Data, but you may not be able to access certain features or view certain content. You have the following choices regarding the Personal Data we process, however, please note that we may not be required to agree to a requested restriction to the extent permitted by law:

**5.2.1 Data Collection & Sharing:** You may generally control how Personal Data is shared with us, and how we share your Personal Data. You can control what Personal Data we collect by modifying Permissions you grant to Providers or by modifying your authorizations to share data with third parties. Additionally, you may change your authorization for our Services to continuously import new contents into your RK360 Record via APIs through tools our Services offer. You may also limit sharing of any Health Records and Health Profile Data, as well as any other Personal Data (including data shared with third parties and subordinate Users) through tools our Services offer.

Please note: Only Account Administrators may control the Permissions of subordinate Users through tools our Services offer. You may contact us through Get in Touch channels (Section 2.2.4) for guidance about how to employ tools our Services offer, but we cannot utilize these tools on your behalf.

**5.2.2 Consent:** If you consent to any other processing of your Personal Data, you may withdraw your consent at any time.

Please note: Your sole means of revoking consent may be to delete your RK360 Record and the Records you administer for others.

**5.2.3 Direct Marketing:** “**Direct Marketing**” means messages to you about offerings unrelated to our Services and Subscriptions. You may have a legal right in certain circumstances not to receive Direct Marketing messages, in which case, you will only receive Direct Marketing messages if you consent or opt-in via links in such messages.

Please note: Messages to you about our Services and Subscriptions do not constitute Direct Marketing. Your sole means of revoking consent to such messages may be to delete your RK360 Record and the Records you administer for others.

**5.2.4 Cookies & Similar Tech:** If you do not want information collected through the use of cookies and similar technologies, you must manage/deny cookies (and certain technologies) using your browser’s settings menu. You must opt out of third-party services directly via the third party.

## 6. Your California Rights

The CCPA provides California consumers with specific rights regarding their Personal Data. In addition to the rights outlined elsewhere in the California Privacy Notice and subject to certain restrictions, California residents may also have the right to request: disclosure of Personal Data collected about them; deletion of Personal Data collected from or maintained about them; and opt-out of sale of Personal Data about them, if applicable.

## 6.1 Request for disclosure of Personal Data collected about you

As stated in Section 5.1.6 of the California Privacy Notice: Residents of California (and others to the extent required by applicable law) may request a list of Personal Data we have disclosed about you to Third Parties for direct marketing purposes during the preceding calendar year (if any). Please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

As stated in Section 5.1.7 of the California Privacy Notice: To the extent required by applicable law, we will provide you with an accounting of the disclosures of your Health Data or Health Profile Data (if any). To do so, please email us at [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us) to make this request.

Please note: We may withhold some information where the risk to you, to your Personal Data, or to our business is too great to disclose the information.

6.1.1: Once we receive a valid request from you, confirm your identity and authorization, and evaluate and mitigate risks of disclosure, we will disclose to you:

- The categories of Personal Data collected about you
- The categories of sources for the Personal Data we collected
- Our business purpose for collecting that Personal Data
- The categories of third parties with whom we shared that Personal Data
- If disclosed for a business purpose, a list identifying the Personal Data categories that each category of recipient obtained

Please note: California residents may exercise their California privacy rights by submitting a request in writing as indicated in the Contact Us section. For security purposes, we may request additional information from you to verify your identity when you request to exercise your California privacy rights. This information will be used solely to verify your identity in connection with your request and will not be retained. Only you, or a person registered with the California Secretary of State that you authorize with Permissions on your behalf, may make a request related to your Personal Data. You may also make a request on behalf of your minor child.

Once you submit a request to (i) access the categories of Personal Data we have about you or (ii) obtain a copy of specific pieces of Personal Data we have about you, we will verify your identity by matching the information provided in your request with information we may have in our system. Upon successfully verifying your identity, we will provide you with your requested information in a secure, password-protected format. If we are unable to verify your identity, we will notify you. We cannot respond to your request or provide you with Personal Data if we cannot verify your identity or authority to make the request and confirm the Personal Data relates to you.

## 6.2 Request for deletion of Personal Data collected from or maintained about you.

As stated in Section 5.1.3 of the California Privacy Notice: Our Services offer you tools, consistent with your Permissions as a User, for deletion of Health Records, Health Profile Data, account registration data and other contents of RK360 Records. You may not, however, delete the Audit Logs that document User activities on the Service and in RK360 Records. We will explain how to

use these tools but cannot utilize these tools on your behalf.

Please note: we store and display copies of Health Records that are maintained in Providers' systems if they are shared with us; we do not control and cannot delete Health Records stored in Providers' systems. Please contact relevant Providers to exercise your right to delete your primary Health Records from their systems.

6.2.1 You may not delete Personal Data if retaining the information is necessary for us or our Services providers to:

- Complete the transaction for which we collected the Personal Data, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities
- Debug products to identify and repair errors that impair existing intended functionality
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law
- Comply with California Electronic Communications Privacy Act (Cal. Penal Code §1546 seq.)
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us
- Comply with a legal obligation
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it

### 6.3 Request for disclosure of sale of Personal Data

As stated in Section 7.1 of this California Privacy Notice and in Section 4.1 of our Terms of Service, we do not sell personally identifiable User Data or RK360 Record Contents including for targeted marketing. Therefore, the right to request such disclosure is not applicable.

## 7. Security

We are required by law to maintain the privacy of your Health Records and Health Profile Data, and we implement reasonable and appropriate security measures to safeguard the Personal Data you provide us. However, we sometimes share Personal Data with third parties as noted above, and we do not have control over third parties' security processes. Further, certain methods of sharing your Health Records you may choose to use may present risks to the confidentiality of Sensitive Personal Data. We do not warrant perfect security and we do not provide any guarantee that your Personal Data or any other information you provide us will remain secure, nor will we be liable for any unauthorized disclosures that occur following your choice to share Personal Data with Users or

recipients you designate, such as Providers. We will notify you if there is a breach of the security of unsecured Personal Data we may process, where such notice is required by law.

7.1 No Data Selling: As stated in Section 4.1 of our Terms of Service, we do not sell personally identifiable User Data or RK360 Record Contents including for targeted marketing.

## 8. Non-Discrimination

RedKangaroo will not discriminate against you for exercising any of your CCPA rights.

## 9. Other California Privacy Rights

In addition to the rights described above, California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Website and Services that are California residents to request certain information regarding our disclosure of Personal Data to third parties for their direct marketing purposes. To make such a request, please send an email to [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us).

## 10. Updates to this California Privacy Notice

As stated above, Prosocial reserves the right to change or modify the Terms of Service, the Privacy Policy, this California Privacy Notice or any policy, procedure, or guideline of the Site, Platform, Services, Records, or Subscriptions (collectively Changes) at any time. If, when you became a Subscriber or a User, you supplied us with your email address, we will notify you at that email address of any material Changes, which will be effective immediately upon implementation of Changes and upon active notification of Subscribers and Users. It is your responsibility to correct and/or update the email address in our files, to assure your timely receipt of notifications about Changes and other matters. Your continued use of the Site, Platform, Services, Records or Subscriptions following the posting or implementation of Changes will confirm your acceptance of such Changes. If the Changes are not acceptable to you, your only option is to stop using the Site, Platform, Services, Records; cancel Subscriptions; export data from Records to storage devices you control; authorize deletion of Records; and uninstall associated mobile and web apps from your devices and computers.

## 11. CONTACT US

By Postal Mail:

Chief Technology Officer

Prosocial Applications, Inc.

1905 15th St. #4585

Boulder CO 80302-4585 USA

By email: [privacy@redkangaroo.us](mailto:privacy@redkangaroo.us)