

SAIGEWARE, INC.**PATIENT USER PRIVACY POLICY**

This notice describes how Personal Data (defined below) and/or medical information about you may be used and disclosed and how you can obtain access to this information. Please review it carefully

INTRODUCTION

We at Saigeware, Inc. (“we”, “us”, “our”, the “Company”, or “Saigeware”) value your privacy and are committed to keeping your personal data confidential. We supply the SAIWELL mobile app (the “App”), and a **BP Monitor, Pulse Oximeter, Digital Thermometer, Peak Flow Meter, Hearing-Aid Devices with Sensors, Gateway Device and/or other medical devices** (“Devices”) as prescribed to patients (each, a “Patient User”) by their healthcare provider (each, a “Provider User”) to support the provision of remote patient monitoring (“RPM”) services. The RPM services, App, Devices, and all associated services are collectively referred to as the “Services.” If you are reading this Patient User Privacy Policy, you are a Patient User.

Patient User Privacy Policy Applicability

This Patient User Privacy Policy applies to personal data that we collect from Patient Users of the Services (“Personal Data”). ***The term “Personal Data” includes any information that can be used on its own or with other information in combination to identify or contact one of our users.*** Some of the Personal Data we collect and transmit may be considered “health data” (i.e., data related to your physical or mental health), “protected health information” or “PHI” (i.e., information that relates to your past, present, or future physical or mental health or condition(s); the provision of health care to you; or the past, present, or future payment for the provision of health care to you), and/or medical records as defined by state law.

We believe that privacy and transparency about the use of your Personal Data are of utmost importance. Therefore, our privacy practices are intended to comply with the Health Insurance Portability and Accountability Act (“HIPAA”) and relevant state law related to the use and disclosure of medical records, where applicable. Additionally, in this Patient User Privacy Policy, we provide you detailed information about our collection, use, maintenance, and disclosure of your Personal Data. The Patient User Privacy Policy explains what kind of information we collect, when and how we might use your Personal Data, how we protect Personal Data, and your rights regarding your Personal Data.

For additional information related to how we use and disclose your Personal Data, health data, PHI, and/or medical records data, ***please contact our Privacy Officer at cpo@saigeware.com.***

Note regarding third-party sites: Our Services may contain links to other sites that we do not own or operate. If you click a third-party link, you will be directed to that third party’s site. We strongly advise you to review the privacy policy(ies) of every site you visit. We have no control over and assumes no

responsibility for the content, privacy policies, or practices of any third-party sites or services. ***This Patient User Privacy Policy does not apply to your use of or access to any third-party sites or services.***

Agreement to Patient User Privacy Policy Terms

BY ACCESSING AND/OR USING THE SERVICES, **YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND AGREE TO THE TERMS OF THIS PATIENT USER PRIVACY POLICY.** IF YOU DO NOT AGREE, YOU MUST IMMEDIATELY CEASE USING THE SERVICES AND THE APP.

Patient User Privacy Policy Updates

Please note that we ***occasionally update this Patient User Privacy Policy, and it is your responsibility to stay up to date with any amended versions.*** Any revisions to the Patient User Privacy Policy will be notified via email. Any changes to this Patient User Privacy Policy will be effective immediately upon providing notice via email and will apply to all Personal Data that we maintain, use, and disclose. If you continue to use the Services following such notice, you are agreeing to those changes.

Account Deletion

If at any point you no longer agree to the use and disclosure of Personal Data, as described in this Patient User Privacy Policy, you can delete your user account on the App ("**User Account**") by sending a deletion request to support@saigeware.com with the following information:

- Your login email address; and
- A statement that you are requesting account deletion.

Questions or Concerns

If you have any questions or concerns after reading this Patient User Privacy Policy, please do not hesitate to contact us at support@saigeware.com. We appreciate your feedback.

COLLECTION AND USE OF PERSONAL DATA

What Personal Data Do We Collect?

We collect five types of information from Patient Users: (i) demographic data; (ii) device data; (iii) self-reported medical data; (iv) support data; and (v) technology data. Each category of data is explained in depth below.

Demographic Data: We collect demographic data from Patient Users, which may include, but not be limited to, your name, date of birth, gender, height, weight, phone number, and e-mail address. The collection of this demographic data is primarily used to provide your designated Provider User with information about you and to provide you with the Services.

Device Data: We will collect information about your condition from a connected blood pressure cuff, blood glucose monitor, digital weight scale, pulse oximeter, temperature, hearing aid sensors, and/ or other medical devices. We collect this information to provide you with the Services and to provide your designated Provider User with the information necessary to monitor and analyze your health condition.

Self-Reported Medical Data: In addition to demographic information, we will collect information regarding your health conditions, including, but not limited to images, 3D face mesh data obtained via the iOS truedepth API, age, gender, weight, height, medical history, and symptoms. We collect this information to provide you with the Services and to provide your designated Provider User with the information required to provide medical treatment to you.

Support Data: If you contact us for support or to lodge a complaint, we may collect technical or other information from you through log files and other technologies, some of which may qualify as Personal Data (e.g., IP address). Such information will be used for the purposes of troubleshooting, customer support, software updates, and improvement of the related Services in accordance with this Patient User Privacy Policy. Calls with Us may be recorded or monitored for training, quality assurance, customer service, and reference purposes.

Technology Data: We use common information-gathering tools, such as log files, cookies, web beacons, and similar technologies to automatically collect information, which may contain Personal Data from your computer or mobile device as you interact with emails or other communications we send you. The information we collect may include your IP address (or proxy server), device and application identification numbers, location, browser type, Internet service provider and/or mobile carrier, the pages and files you viewed, your searches, your operating system and system configuration information, and date/time stamps associated with your usage. This information is used to analyze overall trends, help Us provide and improve our Services, and ensure the proper functioning and security of the Services.

How Will We Use Your Personal Data?

We process your Personal Data based on legitimate business interests, the fulfillment of our Services to you, compliance with our legal obligations, and/or your consent. We only use or disclose your Personal Data when it is legally mandated or where it is necessary to fulfill those purposes described in this Patient User Privacy Policy. Where required by law, we will ask for your prior consent before disclosing your Personal Data to a third party.

More specifically, we process your Personal Data for the following legitimate business purposes:

- To provide the Services;
- To fulfill our obligations to you under the Patient User Terms of Use;
- To properly store and track your data within our system;
- To respond to lawful requests from public and government authorities, and to comply with applicable state/federal law, including cooperation with judicial proceedings and court orders;

- To protect our rights, privacy, safety, or property, and/or that of you or others by providing proper notices, pursuing available legal remedies, and acting to limit our damages;
- To handle technical support and other requests from you;
- To enforce and ensure your compliance with our Patient User Terms of Use or the terms of any other applicable services agreement we have with you;
- To manage and improve our operations and the Services, including the development of additional functionality;
- To manage payment processing;
- To evaluate the quality of service you receive, identify usage trends, and improve your user experience;
- To send you information about changes to our terms, conditions, and policies;
- To allow us to pursue available remedies or limit the damages that we may sustain; and
- To enable you to share Personal Data with your designated Provider User, which enables that Provider User to monitor your progress and overall condition as he/she deems appropriate.

Does We Use Personal Data for Analytics?

We use third-party service providers to monitor and analyze the use of our Services. The analytics services we use may include, but are not limited to google analytics and google cloud platform.

Where Is Personal Data Processed?

The Personal Data we collect through the Services will be stored on secure servers in the United States. Personal Data may be transmitted to third parties, which parties may store or maintain the data on their secure servers. These third parties are not permitted to transfer your Personal Data outside of the United States.

With Whom Do We Share Personal Data?

We may share your personal information with the following categories of individuals/entities:

Business Partners and Vendors: We share Personal Data with a limited number of partners, service providers, and other persons/entities who help run our business ("**Business Partners**"). Specifically, we may employ third-party companies and individuals to facilitate our Services, provide Services on our behalf, perform Service-related functions, or assist us in analyzing how our Services are used. Our Business Partners are contractually bound to protect your Personal Data and to use it only for the limited purpose(s) for which it is shared. Business Partners' use of Personal Data may include, but is not limited to, the provision of services such as data hosting, IT services, customer services, and payment processing.

Our Advisors: We may share your Personal Data with third parties that provide advisory services to us, including, but not limited to, our lawyers, auditors, accountants, and banks (collectively, "**Advisors**"). Personal Data will only be shared with Advisors if we have a legitimate business interest in the sharing of such data.

Provider Users: To use the Services, Patient Users must be affiliated with one or more Provider Users. As part of the Services, we will share your Personal Data with your specified Provider User(s). If at any point you want to deny access to one or more Provider Users, you can do so by emailing support@saigeware.com.

Third Parties Upon Your Direction or Consent: You may direct us to share your Personal Data with third parties. Upon your request and consent, we may share such Personal Data with those third parties that you identify.

Third Parties Pursuant to Business Transfers: In the event of a reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our corporate entity, assets, or stock (including in connection with any bankruptcy or similar proceedings), we may share your Personal Data with a third party.

Government and Law Enforcement Authorities: If reasonable and necessary, we may share your Personal Data to (i) comply with legal processes or enforceable governmental requests, or as otherwise required by law; (ii) cooperate with third parties in investigating acts or omissions that violate this Patient User Privacy Policy or the Patient User Terms of Use; or (iii) bring legal action against someone who may be violating the Patient User Terms of Use or who may be causing intentional or unintentional injury or interference to the rights or property of us or any third party, including other users of our Services.

How Long Do We Retain Personal Data?

We retain your Personal Data only as long as necessary and as required for our business operations, the provision of Services, our contractual obligations, archival purposes, and/or to satisfy legal requirements. The exact period of retention will depend on: (i) the amount, nature, and sensitivity of the Personal Data; (ii) the personal risk of harm for unauthorized use or disclosure; (iii) the purposes for which we process your Personal Data, including whether those purposes can be achieved through other means; and (iv) business operations and legal requirements. In general, we strive to retain your data for no longer than 6 months after your Account is closed (the “**Retention Period**”); however, the above factors may extend or decrease this Retention Period.

At the end of the applicable Retention Period, we will remove your Personal Data from our databases and will require that our Business Partners remove any identifiable Personal Data from their databases. If there is any data that we are unable to delete entirely from our systems for technical reasons, we will put in place appropriate measures to prevent any further processing of such data. ***Please note that once we disclose your Personal Data to third parties, we may not be able to access that Personal Data and we cannot force the deletion or modification of such information by third parties.***

Subject to certain restrictions that may be placed on us by your healthcare provider, we and our Business Partners reserve the right to continue using certain de-identified data indefinitely, even after Personal Data has been removed from our databases. We may continue to disclose de-identified data to third

parties in a manner that does not reveal personal information, as described in this Patient User Privacy Policy. Our continued use of de-identified data will comport with applicable law.

What Happens to Personal Data Submitted by Minors?

We do not knowingly collect Personal Data from individuals under the age of 18 without the consent of the adult responsible for the minor. Additionally, our Services are not directed to individuals under the age of 18. We request that these individuals not provide Personal Data to us. If you are aware of a user under the age of 18 that has provided us with Personal Data without the consent of the adult responsible for that minor, please contact us at support@saigeware.com and we will remove that information and terminate the applicable account.

PATIENT USER RIGHTS***What Rights Do Patient Users Have Concerning Their Personal Data?***

As a user of the Services, you have certain rights relating to your Personal Data. These rights are subject to local data protection and privacy laws, and may include the right to:

- Access Personal Data we store;
- Erase/delete your Personal Data, to the extent permitted by applicable data protection and privacy laws and to the extent technologically feasible;
- Receive communications related to the processing of your Personal Data;
- Restrict the processing of your Personal Data to the extent permitted by law;
- Object to the further processing of your Personal Data, including the right to object to marketing;
- Request that your Personal Data be transferred to a third party, if possible;
- Receive your Personal Data in a structured, commonly used, and machine-readable format; and/or
- Rectify inaccurate personal information and, taking into account the purpose of processing the Personal Data, ensure it is complete.

Where our processing of your Personal Data is based on consent, you have the right to withdraw that consent at any time. If you would like to withdraw your consent or exercise any of the above rights, please contact us at support@saigeware.com.

How Can Patient Users Update, Correct, or Delete Personal Data or Their User Account?

You have the right to request restrictions on the uses and disclosures of your Personal Data. While we are not required to agree to all restriction requests, we will attempt to accommodate reasonable requests when appropriate.

You may change your email address and other contact information by accessing your User Account. If you need to make changes or corrections to other information, you may contact us at support@saigeware.com. In order to comply with certain requests to limit use of your Personal Data, we

may need to terminate your ability to access and/or use some or all of the Services. BY REQUESTING TO LIMIT USE OF YOUR PERSONAL DATA OR DELETE PERSONAL DATA, YOU ACKNOWLEDGE AND AGREE THAT WE WILL NOT BE LIABLE TO YOU FOR ANY CORRESPONDING LIMITATION IN THE SCOPE OF SERVICES OR TERMINATION OF SERVICES AS NECESSARY TO COMPLY WITH YOUR REQUEST.

Should you decide to delete your User Account entirely, you may do so by emailing support@saigeware.com. By terminating your User Account, you agree that you will not be able to access any information previously contained in your User Account. You further understand that it may not be technologically possible to remove all of your Personal Data from our systems. While we will use reasonable efforts to remove your Personal Data, the need to back up our systems to protect information from inadvertent loss means a copy of your Personal Data may exist in a non-erasable form that will be difficult or impossible for us to locate or remove.

PROTECTION OF PERSONAL DATA

Is Personal Data Secure?

We understand the importance of data confidentiality and security. We use a combination of reasonable physical, technical, and administrative security controls to (i) maintain the security and integrity of your Personal Data; (ii) protect against any threats or hazards to the security or integrity of your Personal Data; and (iii) protect against unauthorized access to or use of such information in our possession or control that could result in substantial harm to you.

While we use reasonable security controls, WE CANNOT GUARANTEE OR WARRANT THAT SUCH TECHNIQUES WILL PREVENT UNAUTHORIZED ACCESS TO YOUR PERSONAL DATA. WE ARE UNABLE TO GUARANTEE THE SECURITY OR INTEGRITY OF PERSONAL DATA TRANSMITTED OVER THE INTERNET, AND THERE IS NO GUARANTEE THAT YOUR PERSONAL DATA WILL NOT BE ACCESSED, DISCLOSED, ALTERED, OR DESTROYED BY BREACH OF ANY OF OUR PHYSICAL, TECHNICAL, OR ADMINISTRATIVE SAFEGUARDS. ACCORDINGLY, WE DO NOT AND CANNOT ENSURE OR WARRANT THE SECURITY OR INTEGRITY OF ANY PERSONAL DATA YOU TRANSMIT TO US. **YOU ASSUME THE RISK THAT UNAUTHORIZED ENTRY OR USE, HARDWARE OR SOFTWARE FAILURE, AND OTHER FACTORS MAY COMPROMISE THE SECURITY OF YOUR PERSONAL DATA AT ANY TIME.**

What Safeguards Do We Have in Place to Secure Personal Data?

We store Personal Data on secured servers and uses a combination of technical, administrative, and physical safeguards to protect your personal information. Such safeguards include, but are not limited to, user authentication, encryption, backups, and access controls.

How Can Patient Users Protect Their Personal Data?

You are solely responsible for preventing unauthorized access to your devices and your User Account by protecting your account credentials and limiting access to your devices. We have no access to or control over your device's security settings, and it is your responsibility to implement any device-level security

features and protections you feel are appropriate (e.g., password protection, encryption, remote wipe capability). We recommend that you take all appropriate steps to secure any device that you use to access our Services and App.

Please note that we will never send you an email requesting confidential information, such as account numbers, usernames, passwords, or Social Security Numbers. If you receive a suspicious email from us, please notify us at support@saigeware.com.

Further, if you know of or suspect any unauthorized use or disclosure of your User Account information or any other security concern, please notify us immediately.

What If We Experience a Data or Security Breach?

We take the security of your Personal Data seriously. In the event of a data or security breach, we will take the following actions: (i) promptly investigate the security incident, validate the root cause, and, where applicable, remediate any vulnerabilities within our control which may have given rise to the security incident; (ii) comply with laws and regulations directly applicable to us in connection with such security incident; (iii) as applicable, cooperate with any affected user or client in accordance with the terms of our contract with such user or client; and (iv) document and record the actions we take in connection with the security incident and conduct a post-incident review of the circumstances related to the incident and actions/recommendations taken to prevent similar security incidents in the future. We will notify you of any data or security breaches as required by and in accordance with applicable law.

COMMUNICATIONS

Can Patient Users Opt Out of Receiving Communications from Us?

We may send communications, including emails, to you regarding your User Account and the Services or App. You can choose to filter any User Account, Services, and App emails using your email settings, but we do not provide an option for you to opt out of these communications.

If you consent to receive marketing or other communications not related to your User Account or the Services/App, we will provide you with the option to opt out of such marketing communications within the applicable message.

What Is Our Cookie Policy?

Cookies are small files that a web server sends to your computer or device when you visit a web application that uses cookies to keep track of your activity on that site. Cookies also exist within applications when a browser is needed to view or display certain content within the application. Cookies hold a small amount of data specific to a web application, which can later be used to help remember information you entered in the application (like your email or username), preferences selected, and movement within the application. We use cookies and other technologies to, among other things, better serve you with more tailored information, and facilitate efficient and secure access to the Services.

Our cookies do not, by themselves, contain Personal Data. Further, we do not combine the general information collected through cookies with any other Personal Data to identify you. However, we do use cookies to identify that your web browser has accessed aspects of the Services and may associate that information with your User Account (if one exists).

Presently, we use Google Firebase, Google Analytics, session cookies, basic user information cookies. In addition, we may also collect information using pixel tags, web beacons, clear GIFs, or other similar technologies. This information may be used in connection with website pages and HTML formatted email messages to, among other things, compile statistics about usage and response rates.

How Can Patient Users Opt Out of Cookies?

If you prefer, you can usually choose to set your browser to remove cookies and reject cookies. If you enable a do not track signal or otherwise configure your browsers to prevent us from collecting cookies, you will need to reenter your login information each time you visit the login page. You may also be unable to take advantage of some of the Services.

Do Not Track Disclosure

Some web browsers may transmit do not track ("DNT") signals to websites with which the user communicates. To date, there is no industry standard for DNT and users cannot know how a given company responds to a DNT signal they receive from browsers. We are committed to remaining apprised of DNT standards. However, we do not support DNT browser settings and does not currently participate in any DNT frameworks that would allow us to respond to signals or other mechanisms regarding the collection of your personal information.

CALIFORNIA PRIVACY RIGHTS

If you are a California resident, the California Consumer Privacy Act ("CCPA") may apply to you. Please see the CCPA Attachment for an explanation of your rights.

Under California Civil Code sections 1798.83-1798.84, California residents are entitled to ask for and obtain from us an annual list identifying the categories of personal customer information which we shared, if any, with our affiliates and/or third parties in the preceding calendar year for marketing purposes. This list will be provided free of charge. Contact information for such affiliates and/or third parties must be included. If you are a California resident and would like a copy of this notice, please submit a written request to the following address:

Saigeware, Inc.
450 Sutter St #1400 San Francisco CA 94104
Email: support@saigeware.com

[END]