PRIVACY & SECURITY POLICY

Last updated October 20, 2020

Thank you for entrusting Circadiance LLC ("**Circadiance**", "**we**", "**us**", or "**our**") with your or your patient's information and data. We are committed to protecting their personal information as well as your own. We provide this Privacy & Security Policy to let you know how we will use your patient's information and your information in relation to the monitoring of their health using our equipment and system. If you have any questions or concerns about our policy or our practices with regards to personal information, please contact our Data Protection Officer, Greg Ulery, at greg.ulery@circadiance.com.

Circadiance LLC provides a range of products relating to monitoring and assisting with breathing, cardiovascular health and apnea for adults, children and infants (the "**Monitoring Devices**"). We provide these Monitoring Devices and associated interactive access to our Synergy Cloud service ("**Synergy Cloud,**" "**System**" or "**Services**") to doctors, hospitals and home health companies ("**HHC**") (each individually, "**you**" or "**your**") for distribution of the Monitoring Devices to your patients as prescribed for their use at home as instructed by you or their prescribing physician.

Synergy Cloud includes an Account for each hospital or HHC. Each Account is associated with:

- one or more Users who have password-restricted access to Synergy Cloud for data input, review and interpretation of data, and management of cases associated with that Account, such Users including employees of the hospital, HHC or data scoring and interpretation consultants;
- one or more Cases where each Case corresponds to a different patient; and
- one or more Contacts which may be individuals that receive certain notices regarding associated Cases, such as parents or guardians, and physicians such as referring physicians, prescribing physicians, primary care physicians and specialists.

This Privacy & Security Policy applies to all information collected through the Monitoring Devices or input into Synergy Cloud.

When you prescribe one of our Monitoring Devices or use our Services, you are trusting us with your patients' personal information, including personal health information. We take their privacy very seriously. In this Privacy and Security Policy, we seek to explain to you in the clearest way possible what information we collect, how we use it and what rights there are in relation to it.

Please read this Privacy and Security Policy carefully as it will inform you about using our Monitoring Devices and Services.

1. WHAT INFORMATION DO WE COLLECT?

We may collect both health-related and non-health related information about your patients, as well as identifying information about your patients, their families, and your Users and Contacts as identified in Synergy Cloud for the Monitoring Devices and Services to perform as intended. Collectively, this information is referred to as **Personal Information**.

Patient Personal Health Information

We collect certain personal health information regarding your patients' health and wellness ("**Patient PHI**").

For instance, the Monitoring Devices may collect and report certain Patient PHI to Synergy Cloud, such as vital signs like heart rate or pulse, breathing rate, oxygen levels and/or consumption and apnea events, and sleep information such as sleep cycle and markers thereof ("**Raw Data**"). This may occur during the monitoring or recording operation phases of the Monitoring Devices.

We may collect other Patient PHI from your Users relating to the patient for their Case. This may include personal and family medical history; disease or medical condition diagnoses; prescription information for the Monitoring Device such as instructions for dosage, usage and operation of the Monitoring Devices; biographic information such as age and race; medical test results; allergies and contraindications; and prescriptions.

We may also collect Patient PHI from other Users, such as interpreting physicians or scorers that review and interpret patient Raw Data through Synergy Cloud and may summarize their interpretations in reports for you or the prescribing or treating physician.

Any Patient PHI we collect, regardless of the method of collection, is only collected strictly as necessary for your patients' use of the Monitoring Devices and the Services, as authorized by them with their signing of the Consent Form provided along with the Monitoring Device as confirmed by you.

We abide by the Health Insurance Portability and Accountability Act of 1996, as amended ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act ("**HITECH Act**"), and their regulations for all Patient PHI we collect and store. We specifically follow the standards for privacy and security of individually identifiable health information according to HIPAA.

Personally Identifiable Information

We also collect non-health related personal information that may identify the patients, their parents or guardians, and the Users and Contacts of Synergy Cloud (called Personally Identifiable Information or "**PII**"). We may collect this from you and Users of the Services that you authorize, such as employees and interpreting physicians or scorers, through their use of the Services. These PII may include: contact information such as name, address, email address, nicknames, phone numbers; family member names; login credentials such as usernames and passwords used for

account creation, access and authentication; online identifiers such as IP (Internet Protocol) address, browser and Monitoring Device characteristics, operating system, language preferences, cookies, referring URLs, Monitoring Device name, country, location, and associated accounts.

This information is primarily needed to create and authenticate each User for the Services, maintain the security and operation of the System, improve our Monitoring Devices and System, and for our internal analytics and reporting purposes.

All information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such information.

2. WHAT ARE OUR OBLIGATIONS UNDER HIPAA REGARDING HEALTH INFORMATION?

The Patient PHI we collect and store for you belongs to your patient. We are HIPAA-compliant. This means that, as a Business Associate, we do the following:

- don't use or disclose the Patient PHI other than as permitted or required by the Services or by law (see Section 3 for the permitted uses);
- use appropriate safeguards to prevent the use or disclosure of the Patient PHI other than as required by the Services (see Section 8 for more details);
- report any unauthorized use or disclosure of the Patient PHI to you, including data or security breaches of unsecured protected health information;
- ensure that any Third-Party Service Providers we use that may receive, maintain, or transmit Patient PHI agree to the same restrictions and conditions that apply to us with respect to such information (see Section 6 for more);
- cooperate with you in responding to any privacy requests by the patient or their parent(s) or guardian(s) in the case of minors, regarding their Patient PHI, including: (1) making their Patient PHI available, (2) amending their Patient PHI, and (3) providing an accounting of disclosures of the Patient PHI (see Section 10 for more on privacy requests); and
- make our records relating to the use and disclosure of the Patient PHI available if audited.

3. HOW DO WE USE THE INFORMATION?

We may use your Personal Information for a variety of purposes, such as:

- **To enable Monitoring Device operation and provide Services.** We may use Personal Information in enabling operation of the Monitoring Device, collecting Raw Data and interpretations thereof, and in providing and maintaining Synergy Cloud.

- **To facilitate account creation and login process.** We may use Personal Information to create and maintain secure Accounts and associated Users, Contacts and Monitoring Devices in Synergy Cloud.

- **To manage Users.** We may use Personal Information for the purposes of managing Accounts and Users on Synergy Cloud and keeping it secure and in working order.

- **To enable User communications.** We may use Personal Information to enable communications between authorized and associated Users in Synergy Cloud.

- **To maintain the security of the Synergy Cloud system.** We may use Personal Information to detect, prevent and address technical issues with the Synergy Cloud system.

- **To send administrative information to you.** We may use Personal Information to send you or your Users or Contacts product, service and new feature information; information or updates about replacement parts for the Monitoring Device; and/or information about changes to our terms, conditions, and policies.

- **To respond to user inquiries/offer support to users.** We may use Personal Information to respond to inquiries and solve any potential issues you might have with the use of our Monitoring Devices or Services.

- **Request Feedback.** We may use Personal Information to request feedback on the Monitoring Device or our Services.

Further, we may de-identify Personal Information for certain purposes, such as:

- **Anonymization.** Information that is anonymized no longer identifies its owner. We may use this information for analysis of aggregate data, such as for statistical purposes, Synergy Cloud system performance, and other similar uses. We may also use such anonymized information for any legitimate purpose at our discretion.

- **Pseudonymization.** Information that is pseudonymized has had the identifying portion of the data temporarily masked but can later be re-associated with the corresponding information when necessary. This may be used particularly for Patient PHI to maintain the security of health-related information until association of identity with the information is needed by you. However, according to the terms of the Business Associate Agreement signed with you, **we will not re-associate any de-identified Personal Information, including Patient PHI**.

The Personal Information that we collect may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction. For instance, we store the Personal Information in the United States.

If you are located outside United States and choose to provide information to us, please note that we transfer the data, including Personal Information, to the United States and process it there. This may be done subject to Standard Contractual Clauses according to the GDPR for Personal Information of citizens of the European Union.

4. WILL THE INFORMATION BE SHARED WITH ANYONE?

We do not sell data and will never sell the Personal Information.

We may, however, share Personal Information with certain third parties as follows:

- **Medical Review:** Patient PHI collected through the Monitoring Device will be available to other Users associated with each Account according to the roles of the Users as established in the Synergy Cloud system. For instance, interpreting physicians or scorers associated with a particular Account may review Raw Data from associated Monitoring Devices, and prescribing or treating physicians may have access to reports or summaries of interpretations made by these interpreting physicians or scorers. Only Users associated with a common Account will be able to review Personal Information about Cases, Monitoring Devices, other Users and Contacts that are associated with that Account, according to the established permissions of each role.

- **Legal Obligations:** We may disclose the Personal Information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).

- **Vital Interests:** We may disclose the Personal Information where we believe in good faith it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved. We have been requested to respond to sheriff's requests to analyze data when the local law enforcement officer suspected child abuse. We have complied with those requests.

- **Research:** We may disclose the Personal Information to third parties for use in medical research. If we do so, it will be fully anonymized, so it no longer identifies the underlying individual.

Other than the above, unless otherwise required to do so by law, we will not share the Personal Information with anyone unless expressly authorized to do so by you.

5. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

We may use cookies and similar tracking technologies (like web beacons and pixels) in Synergy Cloud to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

6. WHAT IS OUR STANCE ON THIRD-PARTY SERVICE PROVIDERS?

We may use certain third-party cloud hosting service provider(s) to hold the Personal Information securely in the cloud. We may also use third-party service providers to assist with information technology, email, software or program analytics, and research and therefore may need to share or disclose the Personal Information with them for these purposes. Any third-party access to the Personal Information will be limited to only those third parties and only as needed to perform these tasks on our behalf. They are obligated not to disclose or use it for any other purpose.

They have also agreed to follow the requirements of this Privacy & Security Policy and to use physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Patient PHI as required by HIPAA and the HITECH Act.

We are not responsible for the content or privacy and security practices and policies of these third-party providers. You should carefully review their privacy policies and other conditions of use. More information may be found here.

By using the Services (or by using the Monitoring Device if you are a patient or parent/guardian of the patient), you are agreeing that the Personal Information may be shared with these third parties for these purposes.

7. HOW LONG DO WE KEEP THE INFORMATION?

We will only keep PII for as long as it is necessary for the purposes set out in this Policy, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements). When we have no ongoing legitimate business need to process the PII, we will either delete or anonymize it, or, if this is not possible (for example, because the PII has been stored in backup archives), then we will securely store the PII and isolate it from any further processing until deletion is possible.

However, United States law requires that we retain all medical data, including Patient PHI, once it is collected. We may securely store the Patient PHI and isolate it from the remainder of data through encryption, firewalls, dedicated silos and other appropriate data security measures in

compliance with HIPAA regulations. The Patient PHI data may be stored in de-identified or pseudonymized form. We may, at our discretion, archive Case information, including Raw Data and other Patient PHI, periodically.

8. HOW DO WE KEEP THE INFORMATION SAFE?

We are required by law to maintain the privacy and security of the Personal Information, especially the Patient PHI.

To do this, we have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we collect and hold. These measures may include:

- secure hosting of data with reputable cloud-based hosting service providers that are also required to take appropriate security measures under HIPAA;
- firewalls;
- maintaining all Patient PHI in a secured location separate from other Personal Information;
- encryption and de-identification;
- controlling access through strong passwords and two-factor authentication for all Users;
- audit trails for access and activity;
- encoding all Personal Information both in transit and at rest using state of the art data encryption algorithms for protected health information;
- anti-virus and malware protection; and
- periodic vulnerability and penetration testing.

However, we cannot guarantee 100% security. We will do our best to protect the Personal Information, but in the unlikely event of a data or security breach that affects the Personal Information, especially Patient PHI, we will notify you of the breach and the steps being taken to address it. Similarly, any notification of breach we receive from a Third-Party Provider (such as the cloud hosting service) that affects the Personal Information, especially Patient PHI, will be passed along to you. Third-Party Providers are responsible for the security of their own systems.

In addition, the Monitoring Devices and Synergy Cloud system do not have any malware, bots or malicious programming or code that would introduce vulnerabilities to the security of your information technology system, such as your computer(s), Wi-Fi or other Internet-accessible network.

9. DO WE COLLECT INFORMATION FROM MINORS?

We may collect data from children under 18 years of age, including infants who are being monitored by a Monitoring Device. By using the Synergy Cloud system, you represent that either you or the physician providing the Monitoring Device to the patient have obtained the consent of the patient, or the patient's parent(s) or guardian(s) if the patient is a minor, for the collection of their Patient PHI and other Personal Information through the Monitoring Devices and Synergy Cloud.

If we learn that Personal Information of an individual less than 18 years of age has been collected without the consent of a parent or guardian, we will deactivate the corresponding Monitoring Device, suspend the corresponding Account and take reasonable measures to promptly identify and sequester such data from our records.

If you become aware of any data we have collected from children under age 18 without the consent of a parent or guardian, please contact us at greg.ulery@circadiance.com.

10. RESPONDING TO PRIVACY REQUESTS

Citizens of any Member State of the European Union have certain rights with respect to the processing of their personal data (referred to here as Personal Information) as defined by the Regulation (EU) 2016/679 (General Data Protection Regulation) effective May 25, 2018 ("GDPR").

Natural persons who are residents of the state of California have certain rights under the California Consumer Privacy Act of 2018 (the "CCPA") with respect to their Personal Information.

If you receive any request from a patient, their parent(s) or guardian(s), User or Contact with respect to exercising any of their privacy rights under the GDPR, CCPA or other privacy law, please contact our Data Protection Officer, Greg Ulery, at greg.ulery@circadiance.com or the contact information provided at the bottom of this page. We will work with you to respond to their request.

11. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting that can be activated to signal a privacy preference not to have data about your online activities monitored and collected. We do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online.

12. DO WE MAKE UPDATES TO THIS POLICY?

We may update this Privacy & Security Policy from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this Policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Policy frequently to be informed of how we are protecting the information.

13. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this Policy, you may contact our Data Protection Officer (DPO), Greg Ulery, by email at greg.ulery@circadiance.com, by phone at 724-858-2837, or by post to:

Circadiance LLC
Greg Ulery
1300 Rodi Road
Turtle Creek, PA 15145
United States