PRIVACY POLICY FOR END USERS

Last updated: March 16, 2025

Who we are and what do we do?

We at Itamar™ Medical Ltd. (together with our affiliated companies – "**Itamar Medical**", "**we**", "**us**" or "**our**") develop and operate proprietary medical devices and related mobile applications and web-based platforms for diagnosis and care management of sleep apnea (collectively – our "**Products**"). We provide such Products to our corporate customers and business partners, including hospitals, clinics, and healthcare professionals (collectively – our "**Customer(s)**").

To whom does this policy relate?

This Privacy Policy for End Users ("**Policy**") describes our privacy practices with respect to identified or identifiable information ("**personal data**" or "**personal information**") relating to patients, physicians, and office administrators of our Customers who use the Products at our Customers' direction ("**Patient**", "**Physician**" or "**Admin**", respectively, and collectively – "**End User**" or "**you**").

As further explained in Section 9 below, the responsibility for complying with most legal requirements applicable to a Data Controller (or a Covered Entity under the U.S. Health Insurance Portability and Accountability Act ("**HIPAA**")) with respect to your personal data processed by us, lies with our Customer – typically, the organization providing you with healthcare services as a Patient, or by which you are engaged as a Physician or Admin. In other words, we process your personal data on your healthcare provider's instructions, and are not responsible for its privacy practices. Your healthcare provider may have additional privacy notices explaining its own specific privacy practices, in which case, we encourage you to read them.

Providing your personal data directly to us - a service provider processing personal data on behalf of our Customers - is entirely voluntary and not legally required. However, please keep in mind that without it, the functionality of our Products may be limited or entirely unavailable to you.

Note that this Policy does NOT cover our processing of personal data relating to individuals who interact with Itamar Medical's assets outside the Products (such as our website visitors and business contacts) with regard to whom we act as a Data Controller. To learn more about our privacy practices regarding the personal data of such individuals, please visit our Privacy Policy for Website Visitors and Business Contacts.

Specifically, this Policy describes our practices regarding:

We respect your privacy and are strongly committed to making our practices regarding your personal data transparent and fair. **Please read this Policy carefully and make sure that you fully understand it.**

1. Data Collection

We collect certain types of personal data regarding Patients, Physicians and Admins as instructed by the relevant Customer. Such data is typically generated automatically through your interaction with the Products; collected directly from the Patient or their Physician, including via a Patient screening questionnaire; or from third parties (including Service Providers, defined in Section 5 below) as may be instructed by the Customer who directed you to use our Products.

Specifically, depending on the Products you use and at your Physician's direction, we may collect the following categories of personal data about you:

- **End User Profile:** Full name, government-issued ID or social security number, Customer-issued Patient ID, gender, date of birth or age, PIN code, the Customer and clinic you are associated with, and the referring and interpreting Physician's medical specialty.
- **Contact Details:** Email address, home address, and mobile or landline phone numbers.
- **Delivery Status:** If your healthcare provider is enrolled in our WatchPAT® Direct Program, we may track the location and shipment status of the Product assigned to you to ensure timely delivery to you and (for reusable Products) its return after use.
- **Medical Data:** This may include data collected through the Products, such as Peripheral Arterial Tone signal, heart rate, oximetry, body position, snoring, and chest motions; medical device output (such as AHI); responses from you or your Physician to a patient screening questionnaire regarding your sleep habits and overall health (such as medical history, medications, current or past treatment for high blood pressure, BMI, height, weight, neck size, daytime sleepiness, and observed breath stoppage during sleep). and diagnostic inferences drawn from such data by your healthcare provider.
- **Product Usage Data:** When our U.S. Customers and their End Users use our Products, we collect certain data about these interactions. This includes technical and usage data transmitted by your mobile phone or computer, such as device type and operating system, app version, pages viewed within the app, date and time stamp, Patient screening questionnaire section, module, question and answer, as well as Customer clinic and Patient UUID (unique CloudPAT® identifiers). We use this technical data to enhance customer support for our U.S. Customers and their End Users and to improve our services as they relate to such support activities.
- **Mobile Phone Location:** If you install our WatchPAT® mobile application on a mobile phone that runs Android operating system 11 or lower, we will ask for access to your phone's location data. We only ask for such access because Google requires us to do so in order to enable Bluetooth scans on such phones. We will NOT access or use this location data in any way.

  Additionally, when your first enter the app from any phone and operating system, we will use the IP address of the network your phone is connected to in order to identify your general location (country/state). This is solely for the purpose of providing you with the relevant country code, allowing you to easily submit your phone number on the verification screen, which is optional. This ensures you are matched with the services assigned to you by your healthcare provider.
- **Direct Communications with Us:** If you reach out to us or our authorized Service Providers for technical or professional support, any personal data you provide during these communications will be processed by us. Depending on the instructions of the Customer you are associated with, this may include recordings and transcripts of calls, emails, form submissions, and chats with us. We process this data for technical support, sleep study analysis, training, recordkeeping, and legal-related purposes.

For the purposes of the California Consumer Privacy Act ("**CCPA**"), during the 12 months preceding the last update of this Privacy Policy, we have collected the personal information described above, which falls within these CCPA-defined categories: For Physicians and Admins, "End User Profile" includes Identifiers and Professional or Employment-Related Information, "Contact Details" includes Identifiers, and "Direct Communications with Us" include Audio, Electronic, or Similar Information; For Patients, "Mobile Phone Location" includes Geolocation Data, and, on phones that run Android 10 or 11, Precise Geolocation (which we will NOT use or disclose in any way). For clarity, all other personal data collected from U.S. Patients as described above is governed by HIPAA and not by the CCPA. We do not use or disclose sensitive personal information, as defined by the CCPA, beyond what is necessary to provide and support our Products.

In any event, personal data processed via any of our Products and related support channels, will only be processed by Itamar Medical on behalf of your healthcare provider – our Customer - in accordance with such Customer's instructions and as further agreed upon in our mutually executed Data Processing Agreement or Business Associate Agreement, any other agreements between us and the Customer, and this Policy.

2. Data Uses

In general terms, your healthcare provider may use our Products to process your personal data in order to improve sleep apnea diagnosis and management for its Patients, while offering its Physicians and Admins a secure and user-friendly interface for reviewing and analyzing sleep apnea data, monitoring Patient progress, making informed decisions, and providing effective treatment.

Itamar Medical may process your personal data as is necessary for the performance of our services, and to facilitate, operate and maintain the Products (all in accordance with the instructions provided to us by your healthcare provider in its role as a Data Controller or a HIPAA Covered Entity, as detailed in Section 9); to comply with our legal and contractual obligations; to provide you with customer service and technical support; and to protect and secure our Customers and End Users, our Products, and ourselves.

Additionally, as mentioned in Section 1 above, we will ask for access to your Mobile Phone Location if you install our WatchPAT® mobile application on a phone that runs Android 11 or lower, for the sole purpose of enabling Bluetooth scans as required by Google. This processing is based on our legitimate interests in ensuring the technical functionality of the app on such phones.

We will also use your phone's IP address when you first enter the app from any phone and operating system to identify your general location and provide you with the relevant country code, allowing you to easily submit your phone number on the optional verification screen. If you choose to submit your phone number, we will securely encode (i.e., hash) it and compare it against our list of hashed Patients' phone numbers to match you with the services assigned to you by your healthcare provider. Should you choose not to enter your mobile phone number, you will be required to enter the 4-digit PIN code given to you by your healthcare provider or by us.

We do not sell nor share your personal information for the intents and purposes of the CCPA.

3. Data Location

Itamar Medical maintains global offices and local representatives in various locations worldwide, including but not limited to Israel, the U.S., the UK, and the EU. Your personal data may be accessed from any of these locations (or other locations as reasonably necessary for the Products' activity) by Itamar Medical employees tasked with handling your healthcare provider's data. Such access typically occurs while providing your healthcare provider with customer and clinical support, technical assistance, and similar services.

The Service Providers (defined in Section 5 below) we use to process your personal data on behalf of your healthcare provider, deemed our "Sub-processors" (or our HIPAA Subcontractor Business Associates, as further explained in Section 9 below), are typically located in the U.S. if your healthcare provider is based in the U.S. – or in the EU or the UK if your healthcare provider is based elsewhere.

Local privacy laws may be different in your location. For such data transfers across territories, Itamar Medical and its Service Providers take appropriate measures to protect your personal data, your fundamental rights and freedoms, and the exercise of your rights in accordance with applicable laws.

If we transfer personal data originating from the European Economic Area (EEA), the UK, or Switzerland to countries that provide an adequate level of data protection based on adequacy decisions published by the European Commission, the UK, and Switzerland (as applicable), we rely on these adequacy findings regarding the level of data protection offered by the recipient country.

To the extent we transfer End Users' personal data originating from the EEA, the UK, or Switzerland elsewhere, we and the relevant data exporters and importers rely on appropriate data transfer mechanisms as established under applicable law, such as adequacy decisions, or, when transferring personal data to non-adequate countries, the standard contractual clauses adopted by the EU (available here) or the UK (available here). You can obtain a copy by contacting us as indicated in Section 10 below.

4. Data Retention

We retain your personal data on behalf of your healthcare provider and in accordance with its instructions. We may retain some of your personal data after the termination of our engagement with your healthcare provider, to the extent reasonably necessary for us to comply with our legal and contractual obligations; to perform and enforce our agreements; and to resolve and protect ourselves against legal disputes – all in accordance with our agreements with the relevant Customer, applicable laws and our data retention policies (where applicable).

Please note that except as required by applicable law or our specific agreements with your healthcare provider, we will not be obligated to retain your personal data for any particular period, and are free to securely delete, anonymize or restrict access to it for any reason and at any time, with or without notice to you.

If you have any questions about our retention practices as regards your personal data, please contact your healthcare provider.

5. Data Disclosure

We may disclose your data to certain third parties, including law enforcement agencies and our Service Providers (defined below), in accordance with this Policy and as described below:

- **Service Providers:** We engage selected third-party companies and individuals to perform services complementary to our own. Such service providers may include,

without limitation, hosting and server co-location services, communications and content delivery networks (CDNs), data and cyber security, package delivery and tracking services, customer support call centers, session, call or activity recording and analysis, remote access, performance measurement, customer management systems, and any other relevant service (collectively – our "**Service Providers**").

These Service Providers may have access to your personal data, depending on each of their specific roles and purposes, and may only use the data for such limited purposes as determined in our agreements with them.

- **Customers and their End Users and service providers:** We may disclose your personal data to your healthcare provider (including data and communications concerning your End User Profile, Delivery Status, and Medical Data). In such cases, disclosing such data means that your Physician and/or your healthcare provider's Admins may access your data on behalf of your healthcare provider, and will be able to monitor, process, and analyze it. If so instructed by your healthcare provider, we may also disclose your personal data directly to third-party service providers engaged by your healthcare provider, or receive certain relevant data from your healthcare provider's account on the third-party provider's service.
- **Legal compliance:** In exceptional circumstances, we may disclose or allow government and law enforcement officials access to your personal data, in response to a subpoena, search warrant, or court order (or similar requirement), or in compliance with applicable laws and regulations. Such disclosure or access may occur if we believe in good faith that: (a) we are legally compelled to do so; (b) disclosure is appropriate in connection with efforts to investigate, prevent, or take action regarding actual or suspected illegal activity, fraud, or other wrongdoing; or (c) such disclosure is required to protect our legitimate business interests, including the security or integrity of our Products and related services.
- **Protecting rights and safety:** We may disclose your personal data to others if we believe in good faith that this will help protect the rights, property, or personal safety of Itamar Medical, its employees or stakeholders, any of our End Users or Customers, or any member of the general public.
- **Itamar Medical affiliates and organizational changes:** We may disclose your personal data internally within our group, for the purposes described in this Policy. In addition, if Itamar Medical or any of its subsidiaries or affiliates undergo any change in control or ownership, including by means of merger, acquisition, or purchase of substantially all or part of its assets, your personal data may be shared with the parties involved in such an event. If we believe that such change in control might materially affect your personal data then stored with us, we will notify you of this event and the choices you may have via any communication means available to us.
- **Additional disclosures:** For the avoidance of doubt, Itamar Medical may disclose personal data in additional circumstances, pursuant to your healthcare provider's or your own explicit approval, or if we are legally obligated to do so, or (where applicable) if we have successfully rendered such data non-personal, non-identifiable and anonymous.

For the purposes of the CCPA, in the past 12 months, we may have disclosed Physicians' and Admins' Identifiers, Professional or Employment-Related Information, and Audio, Electronic, or Similar Information, to our Service Providers, Customers and their End Users and service providers, law enforcement officials, our affiliates, and in the context of a change of control. We have not disclosed Patients' personal information that is governed by the CCPA to any third party.

6. COMMUNICATIONS

We may contact you with important information regarding our Products. For example, we may call you on the phone or send you SMS or email notifications to encourage you to use a Product sent to you and offer assistance regarding its use. Your healthcare provider may also send you notifications, messages, and other updates regarding your use of the Products. Depending on the Customer with which you are associated, you may be able to control your communications and notifications preferences by contacting your healthcare provider. However, please note that you will not be able to opt out of receiving certain service communications which are integral to your use of the Products (like Product PIN code allocation).

7. DATA SECURITY

We and our Service Providers implement and maintain systems, applications, and procedures to secure your personal data, and to minimize the risks of personal data theft, damage, loss, or unauthorized access to or use of such data. These measures provide sound industry-standard security. However, please be aware that regardless of any security measures used, we cannot and do not guarantee the absolute protection and security of any personal data stored with us or any third parties (as described in Section 5 above).

8. YOUR RIGHTS

You may have certain privacy rights under the laws that apply to you, including the EU or UK General Data Protection Regulation ("**GDPR**"), HIPAA, the CCPA, and others. Such rights may include the right to know or request access to specific pieces of personal data collected, categories of data collected and sources from whom it was collected, as well as the purposes of collecting it and categories of third parties to whom we have disclosed it; the right to request rectification or erasure of your personal data held with Itamar Medical; the right to restrict or object to the processing of such data; the right to port it; or the right to equal services and prices (e.g., freedom from discrimination) (each to the extent available to you under the laws that apply to you). If you wish to exercise your rights or to make any request or query with regard to your personal data we process on your healthcare provider's behalf, please contact your healthcare provider directly.

9. ROLES & RESPONSIBILITIES

Certain data protection laws and regulations, such as the EU and UK GDPR, CCPA and HIPAA, typically distinguish between two main roles for parties processing personal data: the "Data Controller" (or under HIPAA, the "Covered Entity" and under the CCPA, "Business"), who determines the purposes and means of processing; and the "Data Processor" (or under HIPAA, the "Business Associate" and under the CCPA, "service provider"), who processes the data on behalf of the Data Controller.

Your healthcare provider is the Data Controller (or Covered Entity or Business) of the personal data uploaded or submitted to the Products. Itamar Medical processes such data as the Data Processor (or Business Associate or Service Provider) on behalf of your healthcare provider, in accordance with its instructions, the Data Processing Agreement or the Business Associate Agreement mutually executed by us and your healthcare provider, and any other commercial agreements we have in place with your healthcare provider. For the purposes of Israel's Protection of Privacy Law, your healthcare provider serves as the "Database Controller" responsible for the personal data we process on its behalf. For the name and contact details

of your Database Controller, please refer to the privacy notice provided by your healthcare provider or contact it directly.

Our Service Providers (as defined in Section 5 above), in turn, are Sub-processors (or under HIPAA, our Subcontractor Business Associates) acting under our instructions.

Your healthcare provider is responsible for meeting any legal requirements applicable to a Data Controller (or a HIPAA Covered Entity or a CCPA Business). If you wish to make any requests or queries regarding our processing of your personal data on behalf of your healthcare provider, please contact your healthcare provider directly.

Itamar Medical assumes the role of Data Controller (solely to the extent applicable under law) with regard to your Mobile Phone Location (as defined in Section 1 above) – and with regards to the processing relating to our website visitors and business contacts, as further elaborated in our Privacy Policy for Website Visitors and Business Contacts.

10. Additional Notices & Contact Details

Updates and amendments: We may update and amend this Policy from time to time. The amended version will be effective as of the date it is published. If we believe any substantial changes are involved, we will provide prior notice via any of the communication means available to us. After such notice period, all amendments will be deemed accepted by you.

Our Products are not designed for underage children: We do not knowingly collect personal data from children and do not wish to do so. If we learn that a person who is underage according to the law applicable to them is using the Products, we will attempt to prohibit and block such use and will make our best efforts to promptly delete any personal data stored with us with regard to such a child (except for data that must be retained for legal purposes). If you believe that we might have any such data, please contact us by e-mail at ItamarDPO@zoll.com.

Data Protection Officer: Itamar Medical has a Data Protection Officer (DPO), who monitors and advises on Itamar Medical's ongoing privacy compliance and serving as a point of contact on privacy matters for data subjects and supervisory authorities. If you have any comments or questions regarding this Policy, if you have any concerns regarding your privacy, or if you wish to make a complaint about how your personal data is being processed by Itamar Medical, you can contact our DPO at ItamarDPO@zoll.com.

EU representative: Arazy Group GmbH has been designated as Itamar Medical's representative in the EU for data protection matters pursuant to Article 27 of the GDPR and may be contacted on matters related to the processing of personal data of individuals in the EU. To make such an inquiry, please send an e-mail to one of the following email addresses: Germany@arazygroup.com, miki.m@arazygroup.com.

UK representative: Medes Limited has been designated as Itamar Medical's representative in the UK for data protection matters pursuant to Article 27 of the UK GDPR and may be contacted on matters related to the processing of personal data of individuals in the UK. To make such an inquiry, please send an email to one of the following email addresses: medes@arazygroup.com, miki.m@arazygroup.com.

Additional questions: If you have any comments or questions regarding this Policy, please contact your healthcare provider or contact us at ItamarDPO@zoll.com.