Pulsenmore Privacy Policy

Last updated: December 2025

INTRODUCTION

Pulsenmore Ltd., along with our subsidiaries and affiliates ("Pulsenmore," "we," "us," and "our") respects your privacy and is committed to protecting your personal information. This Privacy Policy ("Policy") describes how we collect, use, and disclose the personal information we receive in the course of providing our products and services (the "Services"), which includes when you visit our website, www.pulsenmore.com, (the "Website"), use the Pulsenmore mobile application (the "App"), use the Pulsenmore ES ultrasound device (the "Device"), access the cloud platform (the "Platform"), or otherwise interact with us directly or indirectly both online or offline.
To review our Consumer Health Data Privacy Policy, please click here.

OUR ROLE AND SCOPE OF POLICY

Certain data protection laws, including the laws in the EU and the US, differentiate between a party that determines why and how personal data is processed (a "Controller") and a party that processes personal data solely on the Controller's behalf and according to the Controller's instructions (a "Processor"). Pulsenmore is a data Controller with respect to certain of the processing activities outlined in this Policy, while it is a data Processor with respect to other processing activities mentioned in this Policy. For those activities for which it is a data Processor, that processing is governed by a separate agreement between Pulsenmore and the Clinician providing the data—nonetheless, we have described that processing activity in this Policy for the sake of transparency. To the extent you have inquiries regarding activities we conduct or personal information we process in our capacity as a data Processor, we request that you make those inquiries directly with your Clinician and we reserve the right to decline to provide substantive responses to the same.

INFORMATION COLLECTION

"Personal information" or "personal data" refers to any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

The personal information we collect about you depends on your relationship with us. For example, we may collect the following personal information in the following contexts:

- **Clinicians:** From our health care provider customers and their representatives ("Clinicians"), we may collect contact and account information such as name, job title, email, phone number, billing address, shipping address, payment information, username, and password. We may collect certain of this information from prospective customers, as well.
    - Lawful basis: We process this personal information as necessary to perform a contract with you or pursuant to our legitimate business interest to engage with prospective customers.

- **End Users:** About end users of our Services (e.g., patients of Clinicians) ("End Users"), we may collect contact and account information such as name, email, phone number, billing address, shipping address, payment information, username, and password, as well as health information including Protected Health Information ("PHI") such as information regarding their date of birth, pregnancy, prescription, Device, pseudonymized patient ID, answers to clinic questionnaires,

ultrasounds and related metadata, and user feedback and support communications. We may collect this information directly from the End User as well as from their Clinician.
    - Lawful basis: With the exception of user feedback or support communications, we typically process this information in our capacity as a Processor (and in some cases, as a business associate under HIPAA), but in some situations we may be a Controller (e.g., with respect to e-commerce data). We process user feedback and support communications based on your consent and our legitimate interests to improve our Services.

- **Website and App visitors:** About visitors to our Website and App, we may automatically collect information about your computer or mobile device and your user activity, including log data. Some of this information (e.g., IP addresses and device IDs) may constitute personal information. This is discussed further below in the Cookies & Tracking Technologies section below.
    - Lawful basis: We process this personal information for our legitimate interests to perform analytics and advertising about our Services, and in some cases, pursuant to your consent.

- **Job applicants:** About job applicants, we collect contact information, employment and education information, and other information provided on a resume or during the hiring process. We may also collect protected classification characteristics and citizenship information during the hiring process.
    - Lawful basis: We process this information based on our legitimate interest to attract job candidates, and in some cases, pursuant to your consent.

- **Investors and prospective investors:** About investors and prospective investors, we may collect name, professional affiliation, and financial information.
    - Lawful basis: We process this personal information for our legitimate interests to provide and grow our Services.

- **Website inquiries and event/webinar attendees:** About these individuals, we may collect name, contact details, and any other information we may request or that you choose to share with us.
    - Lawful basis: We process this personal information for our legitimate interests to provide and grow our Services.

COOKIES & TRACKING TECHNOLOGIES

We may use cookies and similar technologies such as tracking pixels and web beacons on our Website and App (collectively referred to herein as "cookies") to collect user activity information. The information collected by these tracking technologies may include IP address, geolocation data, browser and device characteristics, operating system, language preferences, referring URLs, information about how and when you use the Website, and other technical details. We may use the following types of cookies:

- **Necessary cookies.** These are cookies that are required for the operation of the Website or App.
- **Functional cookies**. These cookies remember choices you make and are used to recognize you when you return to the Website or App.
- **Security cookies.** These cookies can help us identify and prevent security risks on the Website and App. They may be used to store your session information to prevent others from changing your password without your login information.
- **Analytics/Performance cookies**. These cookies collect information about how you use the Website. They allow us to recognize and count the number of visitors and to see how visitors move around within the Website. These cookies may be placed by us or by third parties.
- **Advertising cookies.** These cookies collect information about your browsing activities on the Website in order to understand your interests for marketing purposes. We, or third parties, may

place or recognize these cookies on your browser when you visit certain websites for the purpose of serving you with advertisements regarding our products and services that may be of interest to you (i.e., retargeting). Such cookies may track your browsing habits and activity when visiting our Website and those of third parties.

We use the following third-party Cookies on our Site: Facebook, YouTube, Google Analytics, Instagram, and TikTok. Additionally, HubSpot cookies may be placed in email messages we send in order to track your interaction with such emails.
We will not place any cookies on your browser that are not strictly necessary unless you have first consented to the cookie pop up. The specific names and types of the cookies, web beacons, and other similar technologies we use may change from time to time. You can adjust your cookie settings in your browser settings or by interacting with the cookie pop up which appears when you first visit the Website. Additionally, by changing your device settings, you can prevent your device's ad identifier from being used for interest-based advertising, or you can reset your device's ad identifier. Typically, you can find the ad identifier settings under "privacy" or "ads" in your device's settings, although settings may vary from device to device. Adjusting your preferences as described in this section does not mean you will no longer receive advertisements, it only means the advertisements that you do see will be less relevant to your interests.

Analytics cookies, targeting and advertising cookies, and the user activity information generated from these cookies, are created, stored and/or managed by third party service providers that provide us with web traffic analytics, sales engagement and marketing automation services, such as Google Analytics and others. You can opt-out of Google Analytics by downloading Google's Opt-Out Browser Add-on.

Some internet browsers have "Do Not Track" or "DNT" features which, when turned on, send a signal to a website that the individual visiting the website does not wish to be tracked. Such browser features and industry standards are not uniform, so our Website does not respond to DNT signals, but you can control your cookie preferences in the settings of your Internet browser.

Depending on your state of residence, you may also have the right to opt-out of targeted advertising activities. See further discussion below under the section titled Your Privacy Rights.

INFORMATION USE

We process personal information for a variety of purposes, including to:

- Provide our Services.
- Respond to your questions and otherwise communicate with Clinicians and prospective customers.
- Solicit feedback from Clinicians and End Users.
- Provide patient and customer support and process reports and inquiries related to quality control or returns.
- Operate, manage, and run our business and maintain records.
- Develop, improve, and maintain our Services.
- Analyze and better understand Clinician and End Users' needs, preferences, and interests and conduct analysis and research.
- Advertise and promote our products and Services, including by contacting you to market products, services, and topics that may be of interest to you or otherwise provide you with news, announcements, or updates.
- Collect and analyze information about characteristics and behavior of visitors to our Website and App.

- Undertake quality and safety assurance measures and conduct risk and security controls and monitoring.
- Detect and prevent fraud and perform identity verification.
- Perform accounting, audit, and other internal functions, such as internal investigations.
- Evaluate job applicants for employment.
- Comply with law, regulation, legal process, and internal policies.
- Exercise and defend legal claims.
- For any other purpose you may agree to at or before the time your personal information is collected.

We may also anonymize your personal information (and commit not to attempt to reidentify it) in such a way that you may not reasonably be re-identified by us or any other organization and may use such anonymized information for any purpose. This anonymized data may relate to usage of the App and may also include de-identified ultrasound scans.

INFORMATION DISCLOSURE

We disclose personal information in the following ways:

- **To affiliates and subsidiaries** within our corporate family.
- **To service providers** who process personal information on our behalf, including service providers who provide order fulfillment, data or cloud hosting, information technology support, email hosting, marketing, and analytics services, and other services for the operation of our business.
- To third-party marketing, advertising, analytics, and social media companies, who may process personal information for their own purposes.
- **To your Clinician.** End User personal information, including the user ID assigned to you and the scans conducted through the Device, will be shared with your Clinician. The Clinician serves as a Controller of your data and may use it at its own discretion. For more details on our relationship with the Clinician or about how it uses the data, please contact them directly.
- **To government agencies, law enforcement**, or other relevant parties, such as a law office or independent auditor: (i) if we believe that such disclosure is appropriate to protect our rights, property or safety (including the enforcement of this Policy) or those of a third party; (ii) if required by law or court order; or (iii) as is necessary to comply with any legal and/or regulatory obligations, such as audit or reporting requirements. In particular, we note that in certain circumstances where we are required to provide support services, we may have a regulatory obligation to share certain data with the Ministry of Health.
- **To a successor entity** or purchaser upon a merger, consolidation, or other corporate reorganization in which we participate, or pursuant to a financing arrangement or event of bankruptcy.
- To other third parties with your **consent**.

Pulsenmore does not sell personal information for monetary consideration, though certain of our digital analytics and advertising activities may constitute a “sale” or “sharing” of personal information as those terms are defined under applicable privacy laws (see further discussion in Your Privacy Rights and Additional Information for California Residents sections below).

DATA SECURITY

The security of your personal information is our highest priority. We work hard to make sure that your personal information will be held securely and that it will not be shared or lost accidentally. However, it is impossible to guarantee absolute security. The security of your data also depends on the security of the devices you use and the way in which you protect your user IDs. The measures we take include:

- **Technical Measures**. The electronic safeguards we employ to protect your personal information include secure servers, firewalls, and antivirus protections. We encrypt data in transit and at rest using secure HTTPS protocols.
- **Access Control.** We limit access to your personal information only to authorized personnel who have a need to know. We review these permissions regularly and revoke an employee's access immediately after his/her termination.
- **Internal Policies.** We maintain and regularly review and update our privacy related and information security policies.
- Personnel. We require employees to sign non-disclosure agreements according to applicable law and industry customary practice.
- **Database Backup.** Our databases are backed up and verified regularly. Backups are encrypted and stored within the production environment to preserve their confidentiality and integrity.

As the security of information depends in part on the security of the computer you use to communicate with us and the security you use to protect user IDs and passwords, please take appropriate measures to protect this information.

RETENTION OF PERSONAL INFORMATION

We retain the personal information described in this Privacy Policy for as long as needed to satisfy the purpose for which it was originally collected or for which there is a legitimate business purpose. We determine the retention period for each category of personal information based on: (i) the length of time we need to retain the information to achieve the business or commercial purpose for which it was obtained, (ii) the sensitivity of the personal data, (iii) any legal, regulatory, or contractual requirements applicable to such information, (iv) internal operational needs, and (v) any need for the information based on any actual or anticipated investigation or litigation. Once personal information is no longer needed, we will delete or de-identify it.
Please note that Pulsenmore does not retain ultrasound scans for a prolonged period of time, whether in the App or via the Platform. Thus, we remind Clinicians that they are responsible for downloading and maintaining any ultrasound scans conducted with the Device, and we remind End Users that they should contact their Clinicians regarding access to their data.

THIRD PARTY LINKS

For practical reasons and for your information, our Website may contain links to other websites or services. Pulsenmore exercises no control over such other websites and is not responsible for the content thereon. This Privacy Policy does not apply to third party websites, and we recommend that you review the online privacy policy of any website you visit to determine how the operator handles personal information collected through its website.

CHILDREN'S PRIVACY

Our Services are not intended for use by children under the age of 18 and we do not knowingly collect personal information from children under 18. If we learn we have inadvertently collected personal information from children under 18 years old, we will take steps to delete that information. Pulsenmore does not have actual knowledge that it collects, sells, or shares for cross-context behavioral advertising the personal information of individuals under 18 years of age.

INTERNATIONAL TRANSFERS

Pulsenmore is headquartered in Israel and also operates in the U.S. By using the Services, you acknowledge and agree that your personal information will be processed as set forth in this Privacy Policy, and it may be processed in a country other than your country of residence including the U.S., where laws regarding processing of personal information may be less stringent than the laws in your country. Additionally, some of our service providers may be located in countries other than your own.

- When we transfer your personal information internationally, we will do so in accordance with applicable law. If you are located in the EU, when we share your personal data with third parties based outside of the European Economic Area ("EEA"), we will ensure that a valid transfer mechanism is in place to afford your personal data a similar level of protection as in the EU. For example, we implement the following safeguards:
- When we transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal data such as Israel, we rely on the decision by the European Commission that says that those countries are considered to provide an adequate level of data protection.
- When we transfer your personal information to countries without adequacy decisions, we use specific contracts approved by the European Commission, known as the Standard Contractual Clauses, to give your personal information the same protection it has in the EEA.
- Please contact us at info@pulsenmore.com if you would like further information on the specific mechanism used by us when transferring your personal information out of the EEA.

YOUR COMMUNICATION CHOICES

You may opt-out of receiving promotional or marketing emails from Pulsenmore at any time by using the "unsubscribe" link in the email you receive or contacting us at info@pulsenmore.com. Please note that we reserve the right to continue to send you other non-marketing communications related to your relationship with us.

YOUR PRIVACY RIGHTS

Depending on your state of residence (e.g., the EU, UK, California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia), you may have some or all of the following rights with respect to the personal information we maintain about you. Please note that these rights are not absolute, may apply only in certain circumstances, and we may decline your request as permitted by law. As stated above, please note that requests related to PHI we may process on behalf of your Clinician must be made directly with your Clinician.

- **Right to Confirm / Access / Know.** You may have the right to confirm whether we process your personal information, and the right to request access to and obtain copies of the personal information that we hold about you, including details relating to the ways in which we collect, use, and share your information. In some jurisdictions, you may have the right to know the names of specific third parties with whom we have shared your information. Residents of California have the right to know the categories of personal information we have collected about them, the categories of sources from which the personal information is collected, the categories of personal information sold, shared, or disclosed, the business or commercial purpose for selling, sharing, or disclosing the personal information, and the categories of third parties to whom we have sold, shared, or disclosed their personal information. California's "Shine the Light" law also permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes.

- **Right to Delete.** You may have the right to request that we delete personal information we maintain about you.
- **Right to Correct.** You may have the right to request that we correct inaccurate personal information we maintain about you.
- **Right of Portability.** You may have the right to receive a copy of the personal information we hold about you in a machine-readable format and to request that we transfer it to a third party.
- **Right to Withdraw Consent.** You may have the right to withdraw your consent to the processing of your personal information. This will not affect the lawfulness of any processing prior to such withdrawal.
- **Right to Restrict Processing.** You may have the right to ask us to limit the processing of your personal data. We may continue to use your personal data after a restriction request under certain circumstances.
- **Right to Object to Processing.** You may have the right to object to any processing of your personal data which has our legitimate interests as its legal basis, if you believe your fundamental rights and freedoms outweigh our legitimate interests. If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms.
- **Right to Opt-Out.** You may have the right to opt-out of certain uses of your personal information such as for (i) targeted advertising, (ii) "sale" or "sharing" for cross-context behavioral advertising, or (iii) profiling or automated decision-making activities that result in a legal or similarly significant effect on you. We do not engage in (iii), but you can opt-out of (i) and (ii) by using the mechanisms provided on our Website. Additionally, please note that if you visit our Website with the Global Privacy Control opt-out preference signal enabled, if required by law, we will treat that signal as a request to opt-out of "sale," "sharing," or targeted advertising. Please note your request may only apply to the browser or device from which you submit the request. Learn more about the Global Privacy Control here.
- **Right to Appeal and Lodge a Complaint.** You may have a right to appeal our decision if we decline to process your request in part or in full. You can do so by replying directly to our denial. You also have the right to contact your state Attorney General, or applicable regulator in your jurisdiction of residence such as your European Data Protection Authority, if you have any concerns about how we are processing your personal information, though, we ask that as a courtesy you please attempt to resolve any issues with us first.

Requests to exercise these rights may be made using the contact information listed at the end of this Privacy Policy, or as otherwise described in this section. Only you, or as permitted by law, a person that you authorize to act on your behalf, may make a request related to your personal information. For certain requests, we must verify your request before we can fulfill it. Verifying your request will require you to provide sufficient information for us to reasonably confirm that you are the person about whom we collected personal information or that the requestor is authorized to act on your behalf. We will not discriminate against you for exercising your privacy rights.

ADDITIONAL INFORMATION FOR INDIVIDUALS IN THE EUROPEAN ECONOMIC AREA (EEA), SWITZERLAND, AND THE UNITED KINGDOM (UK)

In addition to the disclosures made elsewhere in this Privacy Policy with respect to our privacy practices, we provide additional disclosures in this section. Our legal basis for processing personal data we collect in the EEA, Switzerland, and the UK can vary depending on the manner in which you use our Services or otherwise engage with us. To the extent we rely on our legitimate interests as a legal basis for processing your personal information, we have considered the balance between our own interests (among other things, the lawful and efficient operation of our Website and Services) and your interests and we believe that (a) you would reasonably expect us to carry out the kind of processing referenced herein, and (b) such processing will not cause you any harm and/or will not seriously impact your rights and freedoms with

regard to data privacy. To the extent we rely on your consent as a legal basis for processing your personal information, you have the right to withdraw such consent given to us for the processing of your personal information at any time, although such withdrawal will not affect the lawfulness of our processing prior to your withdrawal of consent. We may also process personal information where necessary to perform a contract with you, or for our compliance with legal obligations to which we are subject. We also reserve the right to process personal information in the event we believe doing so is necessary to protect the rights of the data subject or another person.

Individuals located in the EEA, Switzerland, or the UK, have the right to access, rectify, or erase your personal data; to restrict or object to processing of your personal data, including automated processing; and to data portability (i.e., the right to receive a copy of your personal data). **As stated above, please note that requests related to health information we process on behalf of your Clinician must be made directly with your Clinician.**

If you have any questions about our privacy practices or wish to exercise these rights, please contact us using the contact information below. You also have the right to file a complaint with your data protection authority if you have a concern about the manner in which we are processing your personal information.

ADDITIONAL INFORMATION FOR CALIFORNIA RESIDENTS

This section provides additional disclosures for residents of California, as required by the California Consumer Privacy Act, as amended (the "CCPA"). Please remember that the information we collect varies based on our relationship with you and note that certain personal information or activities may not be reflected in this section because they are exempt from the CCPA.

CCPA Categories of Personal Information We Collect and How and Why We Collect Them

We collect the following categories of personal information about California consumers. This information may be, or have been, collected directly from the individual, automatically when they use our Services, from third parties such as their Clinician, or from publicly available sources.

- **Identifiers,** including name (first and last), alias, shipping address, billing address, telephone number, business/employment contact information, unique personal identifier, online identifier, IP address, email address, payment card information, health insurance information.
- **Personal Information described in Cal. Civ. Code § 1798.80(e),** including name, signature, address, telephone number, education, employment, employment history, bank account information, credit card number, debit card number, or other financial information.
- **Characteristics of protected classifications** under California or federal law, including age, gender or other demographic information.
- **Commercial information**, including products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- **Internet or other electronic network activity information,** including internet or other similar activity, browsing history, search history, or information about a consumer's interaction with our Website.
- **Geolocation data,** including location data inferred from your device IP address.
- **Audio, electronic, visual, thermal, olfactory, or similar information,** including audio recordings of customer calls or support calls.
- **Professional or employment-related information,** including business contact information as well as information collected from job applicants.
- **Non-public education information**, including transcripts or other information which may be collected during the job application process.

- **Inferences** used to create a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, or attitudes.
- **Sensitive Personal Information,** including account log-in credentials, and personal information collected concerning a consumer's health. We may also collect citizenship information from job applicants. We do not use sensitive personal information to infer characteristics about consumers.

We use and disclose the personal information we collect for the purposes described in the Information Use and Information Disclosure sections above.

CCPA Categories of Personal Information Sold or Shared

Under the CCPA, a "sale" of personal information does not necessarily involve an exchange of money. Instead, a sale also includes disclosures of personal information to third parties who may use the information for their own purposes, such as analytics and advertising cookie providers. Similarly, under California law, "sharing" personal information refers to disclosing personal information to third parties for cross-context behavioral advertising. Per these definitions, we sell and share the following categories of personal information to third party analytics and advertising partners:

- Identifiers
- Personal Information described in Cal. Civ. Code § 1798.80(e)
- Internet or other electronic network activity information
- Geolocation data
- Inferences

Privacy Rights for California Residents Relating to Your Personal Information

Please refer to the Your Privacy Rights section above for information regarding the rights you have with respect to your personal information and how to exercise them.

CHANGES TO THIS PRIVACY POLICY

This Privacy Policy is effective as of the date stated at the top of this page. We may change this Privacy Policy from time to time. When we make changes to this policy, we will post the updated version on our Website and indicate the date the policy was last updated. We encourage you to review this page periodically to check for any updates. Your continued use of our Services indicates your consent to the terms of our Privacy Policy at the time of use.

CONTACT INFORMATION

If you have questions regarding this Privacy Policy or wish to exercise your privacy rights, please contact us at:

Pulsenmore Ltd.
Mail: 8 Omarim St., Omer, Israel, 8496500
Email: info@pulsenmore.com
Website: https://pulsenmore.com/contact/
Phone: (833) 733-2229 (Toll Free)