Privacy Policy

Pre-anesthesia service for patients of hospitals and medical institutions in Israel

Version 1.5 | Updated 11 October 2026

1. Scope of the Policy and the Parties Involved

This policy explains how personal information is handled in the CatAI digital pre-anesthesia service, operated by Cat AI Ltd (the Company), in cooperation with the hospital or medical institution that invited you (the Medical Institution). The policy applies to the service in Israel and does not replace the policy of the marketing website or other services.

For information collected for medical assessment and treatment, the Medical Institution is the database controller when it determines the purposes of processing, and the Company acts as a database holder and processing service provider on its behalf and according to its instructions. For independent operational purposes lawfully determined by the Company, such as handling support inquiries and securing its systems, the Company is the controller of the information for which it is responsible. The allocation of roles reflects actual activities and does not diminish either party's legal obligations.

The name of the Medical Institution and contact methods for the controller of medical information will be displayed in the invitation or application before information is collected. For privacy and information rights inquiries to the Company: service@catai.io. The same address may be used to route an inquiry to the Data Protection Officer, if one has been appointed. Do not send identifying details or medical information that are unnecessary for handling the inquiry.

Personal information means information relating to an identified person or a person who can be identified directly or indirectly, including by combining it with additional information. Medical information is information of special sensitivity under the Protection of Privacy Law. Images, videos, voice and processing results linked to a patient will be treated as personal information even where the patient's name has been replaced with a code.

2. Types and Sources of Information

Depending on the service settings at the Medical Institution, the following are collected: identification and contact details, such as name, identification number, telephone number, date of birth and email address where required; referral, surgery or visit details and associated identifiers; and medical questionnaire answers, including information about illnesses, medications, allergies, medical and functional background and anesthesia history. Facial images, images of the oral cavity and body parts you are asked to photograph, videos and voice recordings are also collected according to the process stages, together with processing results, pathway classification, completion status and medical staff notes and updates. Information is received from you, the Medical Institution and authorized parties involved in the process. Do not photograph other people or include information that is not required.

When contacting the Company or support, the contact details provided, the content of the inquiry and attached documents may also be collected to provide a response, resolve a malfunction and document the inquiry. Provide only information necessary to handle the inquiry.

3. Technical Information and Consent Records

To operate and secure the service and investigate malfunctions, usage and technical data are collected, such as login and activity times, IP address, device type and operating system, application version and error data. The system also records user confirmations, their times and the version of the documents displayed, as well as access and activity data according to the system's mechanisms. Camera and microphone permissions are required for the images and recordings you are asked to provide. Blocking these permissions may prevent completion of the relevant stages. A facial image or voice recording may allow you to be identified even after your name has been removed and is therefore not necessarily anonymous information. The service or an online interface used for it may use cookies, local storage and technical measurement tools for identification, storing preferences, security and operational checks. The types of tools and their use depend on the interface and providers actually used. Tools not necessary to operate the service will be disclosed and addressed separately where required by law. Some tools can be restricted through device or browser settings, but this may affect the operation of the service. Consent to the service does not authorize advertising tracking using medical information.

Device permission to use the camera or microphone does not, by itself, constitute consent to every use of the content collected. Use will be limited to the purposes set out in this policy and to permissions lawfully granted.

4. Purposes of Use and Processing Using Artificial Intelligence

Information is used to identify users and authenticate access, associate the assessment with the correct patient and surgery, collect and present information to the medical staff, generate findings and pathway classifications, transfer information to the Medical Institution and coordinate the subsequent process. Artificial intelligence is used to analyze the required images and recordings and generate preliminary findings. Pathway classification is based on the questionnaire and the Medical Institution's protocol and is not necessarily the output of a machine learning model. Results may contain errors. Performance may vary depending on information quality and patient characteristics. You may ask the Company and the Medical Institution for an explanation of the result and information about documented performance and limitations and may report a concern. Under the Medical Institution's protocol, the questionnaire may result in automatic omission of a separate preliminary visit without individual physician review at this stage.

A physician's examination and medical assessment are still required before surgery. For medical clarification or to request an alternative pathway, contact the Medical Institution. Information is also used for support, operational and quality checks, information security, prevention of misuse, handling inquiries and compliance with legal obligations. These purposes do not authorize unrestricted use of medical information.

5. Choice to Provide Information and Consequences of Refusal

There is no legal obligation to use the application or provide information to the Company through this pathway unless a specific obligation and its legal source are presented to you in advance. Providing information through the digital pathway depends on your willingness and consent. The information required in the questionnaire and image-taking stages is necessary for the digital assessment; without it, the process cannot be completed or a reliable classification obtained.

If you do not consent to providing information, imaging or processing using artificial intelligence, contact the Medical Institution to arrange an alternative pathway, which may include a preliminary visit. Refusing the digital pathway does not automatically cancel surgery and does not waive your right to treatment. Timing and further care will be determined according to medical need and coordination with the institution.

Personal information will be collected and processed on the basis of valid consent or legal authority and within their limits. This document does not create an independent business-interest basis for using medical information. Legal obligations concerning documentation, retention, confidentiality and disclosure may continue after use stops.

6. Recipients of Information

Information and assessment results are provided to the Medical Institution that invited you and its authorized teams for preparation for surgery and treatment. Information may also be accessible to authorized persons at the Company and providers assisting in operating the service, such as storage and cloud, infrastructure, authentication and messaging, technological processing and support providers. Access is granted to the extent required to perform the role and subject to appropriate arrangements. Information may be disclosed under a legal obligation, order or authorized request, or as lawfully required to protect rights and handle a dispute. If the service operator changes, information will be transferred subject to law and continued protection. This policy does not authorize disclosure of medical information to advertisers or data brokers.

Where access by an entity within the corporate group, a professional adviser or an auditor is required, it will be granted only for a defined, permitted purpose and to the extent necessary, subject to appropriate confidentiality and protection obligations. Membership in the corporate group does not itself authorize independent use of medical information.

An engagement with a provider that has access to information or its systems will be governed in accordance with Regulation 15 of the Protection of Privacy Regulations (Data Security), where applicable, including definition of the permitted types of information and processing, confidentiality, security, subcontractors, termination and provider oversight. Providers are not entitled to independently use medical information for advertising or model training on the basis of your consent to this service.

7. Use of Information for Research and Model Training

Your consent to the service is not consent to marketing communications, research outside the service or model training using personal information, including coded information that can be linked to you. Such uses require separate arrangements under law and separate consent where required. Medical research will be conducted only after obtaining the approvals and consents required for the type of research; consent in the application does not replace them.

Statistical data lawfully anonymized may be used for quality control and service improvement after assessing the risk of re-identification. Removing a name alone or replacing it with a code does not make information anonymous. As long as a person can be identified with reasonable effort, personal information protection requirements will apply. The creation of anonymous data itself will take place only within a permitted use of the information.

8. Information Storage and Transfers Outside Israel

Information is stored in the systems used to operate the service and in the Medical Institution's systems to which it has been transferred. Storage location and access options depend on the infrastructure and providers used in the process. If transfer outside Israel is required, including access by a provider outside Israel, it will be subject to the conditions established by law and appropriate protective arrangements. You may contact service@catai.io for information about storage location, provider types and transfers relevant to your process. Storage on a server in Israel does not, by itself, rule out access to or processing of information outside Israel.

Transfers outside Israel will comply with the Protection of Privacy Regulations (Transfer of Data to Databases Abroad), 5761-2001, on the basis of the conditions and undertakings they require. General consent to this policy is not unlimited authorization to transfer information to any country. Storage location, processing providers and access from abroad will be clarified in the relevant service details before obtaining consent on which a specific transfer relies.

9. Information Retention and Deletion

Information will be retained for as long as required for the service purposes, according to its type, the arrangement with the Medical Institution, documentation and inquiry needs and legal requirements. Information transferred to the medical record is also subject to the Medical Institution's retention obligations. Security data, consent records and backups may be retained for periods different from information in active use. Deleting the application from your device does not delete information already stored or transferred. Deletion requests will be considered according to law and retention obligations. There is no commitment to immediate deletion or deletion of a medical record that must be retained. Contact the Company and the Medical Institution to clarify the relevant retention periods.

The Company and the Medical Institution will establish retention periods according to information type and permitted need, review excess information and avoid unjustified indefinite retention. Medical records will be

retained according to the Patient's Rights Law, medical record retention requirements and applicable Ministry of Health guidelines; no single retention period suits all document types. Termination of the service does not authorize a new use of the information.

10. Information Security and Confidentiality

The Company takes organizational and technological measures to protect information and reduce unauthorized access according to its sensitivity and applicable requirements. However, no system is completely immune to malfunctions or security incidents. Security incidents will be handled and reported according to law and the circumstances. Protect your device and access details, do not share a verification code and report suspected unauthorized use. On-screen information, notifications and recordings may be exposed to people nearby. Complete the process in a private place and prevent unauthorized viewing or listening. Precautions taken by you do not replace the information security obligations of the Company and the Medical Institution.

Security obligations apply under the Protection of Privacy Law and the Protection of Privacy Regulations (Data Security), 5777-2017, according to the required security level. As applicable, they include role-based permissions, identification and authentication, access logging, confidentiality duties, protection of information transfers, oversight and incident handling. An allocation of responsibility between the Company and the Medical Institution does not relieve either of its legal obligations. Reports to an authority or notices to patients will be made where required by law or an authorized directive.

11. Your Rights and Contact Methods

Under Section 13 of the Protection of Privacy Law, you may request access to personal information about you held in a database, subject to legal exceptions. Under Section 14, you may request correction or deletion of information that is inaccurate, incomplete, unclear or outdated. The right of access may also apply to images, recordings and results linked to you. Requests will be handled within the timeframes and in the manner prescribed by law.

You may also request deletion or cessation of use. Israeli law does not grant a general, unconditional right to delete all medical information. Requests will be considered according to the circumstances, including retention and documentation obligations. Corrections to a medical record will follow record-management rules, without deleting documentation that must be retained.

Where particular processing is based on consent, you may withdraw that consent for future use. Withdrawal does not invalidate actions lawfully taken earlier or prevent processing required or permitted under legal authority. Ending the digital pathway requires arranging an alternative with the Medical Institution.

To contact the Company: service@catai.io. Identity verification will be required to the extent necessary to handle the request. A request concerning information controlled by the Medical Institution will be referred to or coordinated with it, and you will receive the contact details of the party handling it. You may also contact the Medical Institution to obtain information or a copy of your medical record in accordance with the Patient's Rights Law.

Nothing in this policy restricts contact with the Privacy Protection Authority, the Data Protection Officer if appointed, the person responsible for patient rights at the Medical Institution or a legally competent court or tribunal.

12. Policy Updates

Material changes to the policy or purposes of use will be presented to users appropriately. Renewed consent will be requested where required by law. Publishing a new version does not, by itself, constitute consent to a new use of information already collected. Read this policy together with the Consent and Terms of Use and the Medical Institution's privacy documents, which govern handling of the medical record and the services it provides. If the service links to another party's website or application, handling of information within that service is also subject to that party's policy. Review it before providing information. A link to an external service does not diminish the responsibility of the Company or the Medical Institution for actions within their responsibility.

This policy is governed by Israeli law, including the Protection of Privacy Law, 5741-1981, as amended by Amendment 13, its implementing regulations and the Patient's Rights Law, 5756-1996. Mandatory legal provisions and Ministry of Health requirements prevail over conflicting provisions in this document. This document does not diminish rights that cannot lawfully be waived.