

**“POP” Privacy Policy &
Data Processing Agreement with the surgeon**

A. PRIVACY POLICY

Medacta International SA, with registered offices in Strada Regina, Castel San Pietro (Switzerland) (hereinafter only “Medacta”), in its capacity as data controller regarding the processing of personal data pursuant to UE General Data Protection Regulation 2016/679 (“GDPR”) and to all the applicable privacy laws (hereinafter “Applicable Law”), recognizes the importance of personal data protection and considers that preserving the confidentiality of your personal data is one of the main objectives of its activity.

Before providing any personal data, Medacta invites you to carefully read this privacy policy (“Privacy Policy”), since it contains important information regarding the personal data protection and security measures adopted, in order to ensure confidentiality and full respect of the Applicable Law. Moreover, this Privacy Policy:

- Is to be construed as an information notice, intended for those who interact with Medacta and make use of the services provided by Medacta, like POP;
- Is in conformity with any other Applicable Law related to the minimum requirements for online data collection.

By using the Patient Optimized Pathway Web Application and Mobile App (hereinafter “POP”), you hereby consent to the processing of your personal information in accordance with this Policy. If you do not agree with this Policy, you may not use the POP.

Medacta informs you that processing of your data will be carried out in accordance with the principles of lawfulness, fairness, transparency, accuracy, purpose and storage limitations, data minimisation, integrity and confidentiality. Your personal data will be processed in accordance with the legislative provisions of the Applicable Law and of the confidentiality obligations included therein.

TABLE OF CONTENTS

Please find below the table of contents, which will enable you to quickly track information related to the processing of your personal data.

- 1. DATA CONTROLLER, DATA PROCESSOR AND DATA PROTECTION OFFICER**
- 2. PERSONAL DATA SUBJECT TO PROCESSING**

a Data provided for service performance

a.1. Data Concerning Health

b Browsing data

c Cookies and similar technologies

3. PURPOSES, LEGAL BASIS AND VOLUNTARY OR OBLIGATORY NATURE OF DATA PROCESSING

4. RECIPIENTS

5. TRANSFERS

6. DATA RETENTION

7. ABOUT CHILDREN

8. YOUR RIGHTS

9. PRIVACY OF PATIENT PERSONAL DATA

10. SECURITY

11. AMENDMENTS

12. CONTACT US

1. DATA CONTROLLER, DATA PROCESSOR AND DATA PROTECTION OFFICER

Pursuant to the Applicable Law, Medacta, as POP's developer and owner, is the Data Controller of the data processing activities necessary to provide POP's services and contents.

If You are a healthcare professional, processing personal data through the POP (hereinafter "You" or Your), You shall obtain separate consent from the Patient/Data Subject, as Data Controller. For this data processing, You authorize Medacta as Data Processor for the necessary purposes of technical assistance and maintenance, pursuant to Applicable Law.

This policy describes the extent of the use, protection and precaution Medacta will take in respect of all personal data processed through, or in consequence of, the use of POP.

Medacta has appointed a Data Protection Officer ("DPO") who is freely contactable for any information relating to the processing of personal data by Medacta (e.g., the list of the other data processors) at the following address: privacy@medacta.ch

2. PERSONAL DATA SUBJECT TO PROCESSING

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in

particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person.

By means of POP, Medacta collects the following Personal Data:

a. Data provided for service performance

By means of the POP, You may voluntarily provide Personal data to allow You to make use of the content and services required.

The Personal data processed by the POP may include:

- Name and Surname of patient;
- Contacts;
- Country and date of birth;
- Language;
- Gender;
- Data concerning health (a.1) as requested by You for the medical treatment.

Medacta will process this data and other data necessary for the functionalities of the POP, in accordance with the Applicable Law and on the presumption they refer to you or to third parties who have authorised you to provide them pursuant to an appropriate legal basis which legitimise the processing at stake.

a.1. Data Concerning Health

Medacta, as Developer of POP, does not have access to Data Concerning Health or other Sensitive data of Your Patient, that you process by the POP.

Please note that You shall obtain separate and specific consent from Your Patient to view their information on the POP as permitted by Applicable Law.

You are solely responsible for the Data processing through the POP and for the consent obtained by Your patient for their sensitive data, processed through the POP.

b. Browsing Data

The computer systems and software procedures collect some Personal Data, the transmission of which is an integral part of Internet communication protocols. This information is not collected to be associated with you but, by its very nature, it may allow you to be identified by processing and associating it with data held by third parties. Among collected Personal Data, there are IP addresses or domain names related to the devices used by you to connect to the POP, the URI (Uniform Resource Identifier) of requested resources, the time of the request, the method used to submit the request to the server, the size of the file received as a reply, the numeric code indicating the status of the reply given by the server (successful, error, etc.) and other parameters regarding your operating system and device environment.

This data is used exclusively for the purposes of obtaining anonymous statistics on the use and proper functioning of POP, to control its correct functioning, to enable Medacta to correctly provide the various functionalities to you, as well as for security reasons. This Personal Data may also be used to ascertain any liability in cases of alleged computer crimes against our websites, mobile applications and other tools or against third parties.

c. Cookies and similar technologies

Cookie is a small text file that's stored on your mobile device when you visit POP. Thanks to cookies, POP remembers the actions and preferences (for example, the login data, the preferred language, the font size, other display settings, etc.).

Cookies perform computer authentication, monitoring of sessions and storing information about the activities of users who log onto POP.

Some operations may not be performed without the use of cookies, which in some cases are technically necessary for the operation of the website.

You may find further information on the use of cookie and similar technologies in the Cookie Policy (Section Privacy & Terms).

3. PURPOSES OF THE PROCESSING AND VOLUNTARY OR OBLIGATORY NATURE OF PROVIDING THE DATA

The Personal Data that you provide will be processed by Medacta for the following purposes:

- a) Purposes related to the performance of the POP and necessary to allow You to make use of the content and services required: handle communications between patient and surgeon, exchange contents and direct chat. Medacta may monitor Your usage in order to improve the POP's user experience.
- b) Anonymization of the personal data, in order to conduct research/statistical analyses on aggregated or anonymous data, without the possibility of identifying the data subject, aimed at improving user experience and measuring the functioning of POP;
- c) Purposes related to the compliance with a legal obligation to which the controller is subjected;
- d) Purposes necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

We request your consent for the purpose referred to in point a) and b).

The purpose referred to in point c) does not imply the processing of Personal Data, whilst the processing for the purpose referred to in point d) constitutes a legitimate processing of Personal

Data within the meaning of the Applicable Law because, once the Personal Data has been provided, the processing is indeed necessary to comply with a legal obligation to which Medacta is subject.

Providing your Personal Data for the above-mentioned purposes is voluntary, however, any refusal to provide such data may not allow Medacta to reply to your requests and to comply with legal obligations to which Medacta is subject.

4. RECIPIENTS

Your Personal Data may be disclosed, in close relation to the purposes specified above in section 3, only to:

- a. subjects necessary for order fulfillment of the services (i.e. contractors we use to support our business), in which case we will require such third parties to agree to treat it in accordance with this Privacy Policy and use it for the same purposes. You can obtain the complete list of authorized third parties, by request addressed to DPO at privacy@medacta.ch
- b. persons authorised by Medacta to process Personal Data, that are committed to or under an appropriate statutory obligation of confidentiality (e.g., hosting provider, employees of Medacta) (a. and b. are hereinafter collectively referred to as "Recipients");
- c. law enforcement agencies and public authorities when so required by the Applicable Law.

Medacta guarantees that they will not communicate Your Personal data to non-authorized recipients and will not sell them to anyone.

5. TRANSFERS

Your data will be stored in France. For the purposes described in Section 3, Medacta might transfer some of your Personal Data to Recipients who may be established outside your Country and also outside the European Economic Area. Specifically, Medacta may call upon service providers to supply POP (i.e.: our hosting provider): these third parties may have access to your personal data in the course of providing such services. We require such third parties, who might be based outside the country from which you have accessed to POP, to comply with the Applicable Law in relation to your personal data. Medacta ensures that the processing of Personal Data by these Recipients is carried out pursuant to the Applicable Law. Further details may be requested to the DPO at privacy@medacta.ch

6. DATA RETENTION

Medacta will process your Personal Data only for the duration necessary to achieve the purposes described in section 3. Apart from the above, Medacta will retain your Personal Data for a period of time necessary or permitted to comply with the Applicable Law. Further information regarding the

period of retention of Personal Data and the criteria used to determine such period may be required to the DPO.

7. ABOUT CHILDREN

Medacta will not knowingly collect personally, identifiable information of children under the age of 16, unless with the consent of their parents.

8. YOUR RIGHTS

Pursuant to and to the extent allowed by the Applicable Law, you have the right, at any time, to request, to Medacta, access to, rectification, erasure, restriction of the processing concerning your Personal Data or to object to relevant processing activity and to receive in a structured, commonly used and machine-readable format the Personal Data concerning you.

Requests to exercise your rights must be sent to the following address: privacy@medacta.ch

9. PRIVACY OF PATIENT PERSONAL DATA

Medacta is committed to safeguarding the privacy of patient information - the main end users of POP - and has implemented measures to comply with its obligations under the Applicable Laws, such as pseudonymisation, data encryption, separation of the database storing anagraphic data from the one storing clinical data and other security measures (section 10, SECURITY).

All staff working in Medacta are bound by law and by the Privacy Policy to maintain confidentiality of patient information. If you have a complaint relating to your privacy on the grounds that you believe a health service provider involved in your care has contravened a Privacy Policy, you can contact DPO (section 8, YOUR RIGHTS).

10. SECURITY

Medacta takes reasonable steps to protect personally identifiable information and implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and to protect the information from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. You should keep in mind that no Internet transmission is ever completely secure or error-free.

The security of processing is guaranteed by:

- a) the pseudonymisation and encryption of personal data;
- b) the separation of the anagraphic and clinical data;
- c) the confidentiality, integrity, availability and resilience of processing systems and services;
- d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- e) a regular process of testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

At Your discretion, You can connect by Bluetooth technology to health measuring devices and for any other purpose. If you do not wish to have your personal information transmitted by Bluetooth you may disable Bluetooth on your smartphone or similar device in the settings application for that device, or you may simply not connect (or disconnect if you have already connected) the devices that require Bluetooth.

11. AMENDMENTS

This Privacy Policy came into force on 1st March 2021. Medacta reserves the right to amend or to update its content, whether in whole or in part, including following changes in the legal and regulatory obligations regarding data protection.

In case of such an event, You will be required to accept the new version in order to continue using the POP mobile application. A warning with the new version and acceptance button, will automatically show up during the use of the app.

Furthermore, you will find the updated version of the Privacy Policy in the section Privacy & Terms.

12. CONTACT US

If you wish to request access to the personal data we hold about you or if you have any question, simply contact us:

privacy@medacta.ch

Medacta International SA
Strada Regina CH-6874
Castel San Pietro, Switzerland

B. DATA PROCESSING AGREEMENT

Whereas:

- A Data Controller may engage a Data Processor to carry out processing on behalf of Data Controller.
- The Data Controller shall use only Data Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable privacy laws and must ensure the protection of the rights of the data subject.
- Data Processor must process the personal data only on documented instructions from the controller and must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Medacta International SA will provide the Data Controller with a web application – Patient Optimized Pathway” (“POP”) - that will be used to collect the personal data of patients, pursuant to terms and conditions defined in the document EULA.

Now therefore:

- 1) You (hereinafter “Data Controller”) determine the purposes and the means of the processing of personal data and engage Medacta International SA (hereinafter “Data Processor”), with its offices in Strada Regina, 6874 Castel San Pietro, Switzerland, as Data Processor for all Personal Data Processing performed pursuant to and within the agreements between Data Controller and Data Processor.
- 2) Data Processor performs Personal Data Processing on behalf of the Data Controller with the following purposes:
 - Management and maintenance of the web application provided by Medacta (POP).
 - Anonymization of the personal data, in order to conduct research/statistical analyses on aggregated or anonymous data, without the possibility of identifying the data subject, aimed at improving user experience and measuring the functioning of POP.
- 3) Data Processor must take organizational and technical measures to ensure a level of security appropriate to avoid or reduce the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- 4) Data Processor must take organizational and technical measures (section 3) to ensure:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services;
- the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5) Data Controller guarantees that personal data collected and disclosed to Data Processor by transmission are:

- adequate, relevant and limited to what is necessary for the purposes for which they are processed;
- In any case, personal data and/or data concerning health processed by Data Processor on behalf of Data Controller, are collected and disclosed pursuant to every disposal of Applicable Privacy Law.

6) With this document, Data Controller authorises Data Processor to disclose Personal Data necessary for the performance of a contract to the following categories of recipients:

- Natural or legal persons authorised to access personal data, whose processing is necessary for the performance of a contract to which the Data Controller is party;
- Natural or legal persons authorised to access personal data, whose processing is necessary for compliance with a legal obligation;

7) Data Controller is always responsible for the purposes and means of the processing of personal data through POP.

Data Controller is committed to indemnify Data Processor against all direct costs, expenses, damages, claims, sanctions incurred by Data controller as consequence of a violation of Applicable Law.