PRIVACY POLICY — PATIENT DATA REGISTER

DATA CONTROLLER AND CONTACT PERSON

MEDIPOL OY / CITYKLINIKKA (hereinafter referred to as "City Clinic")
Business ID: 0978621-4
CEO: Piotr Sikorski
Aleksanterinkatu 21 A
00100 Helsinki
+358 (0)201 777 288
info@ckl.fi
The contact persons also include Office Coordinator Tiina Pulliainen and Patient Ombudsman Joonas Jalonen.

REGISTER NAME
Patient Data Register maintained by City Clinic and its independent healthcare practitioners.

PURPOSE OF PROCESSING PERSONAL DATA
The primary purpose of the register is to plan, implement, and monitor patient care, as well as to handle the resulting information. Additionally, the register is used for planning, evaluation, and statistics of the data controller's own operations, as well as for managing the patient relationship. The basis for maintaining the register is the patient or client relationship.

The patient register ensures the supervision of healthcare professionals' activities and compliance with the provisions and regulations related to private healthcare operations. Personal data is processed in accordance with the applicable legislation. The information is treated as confidential.

REGISTER INFORMATION
The register may process the following information about the registered individuals:

• Basic information of the patient/client (name, personal identification number, address, phone number, and guardian for underage patients).
• Patient records and medical information as required by legislation, including:

- Health condition, illnesses, and injuries

- Planning, implementation, and monitoring of examinations and treatments, along with related information
- Laboratory, radiology, and other test results
- Medical opinions and statements

• Photographs
• Name, position, and timestamp of the person making the entry.

REGULAR SOURCES OF INFORMATION
The following are the regular sources of information:

- Information provided by the patient (verified during each visit)
- Information, photographs, reports, and statements generated during the course of treatment
- Other documents obtained with the patient's permission
- Contact requests and image consultation forms received through the website

The processing of the above information is carried out in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679). The information is treated as confidential.

REGULAR DISCLOSURES OF INFORMATION

Patient information is disclosed to the patient themselves unless there is a legal impediment. Based on specific legal provisions, information may be disclosed to authorities and insurance companies.

Notifications of infectious diseases, in accordance with the Communicable Diseases Act (1227/2016), are sent to the regional communicable disease register maintained by the hospital district.

Patient/customer information is disclosed to the adverse drug reaction register maintained by Fimea (Finnish Medicines Agency).
The disclosure of information occurs through paper printouts of electronic patient records and copies of manual materials.
In cases of ongoing care, necessary information may be disclosed to another healthcare facility or healthcare professional for the purpose of arranging the patient's examination and treatment.

In the case of unconsciousness or a comparable condition, information about the patient's identity and health condition may be provided to their close relatives or other individuals close to them, unless there is reason to believe that the patient would object to such disclosure. (Patient Act, Section 13).

Name and contact information are not transferred outside the territory of the European Union member states or the European Economic Area.

PROTECTION OF THE REGISTER

Patient information can only be accessed and processed by healthcare professionals and their assistants who are currently involved in the patient's treatment. Information can only be processed to the extent necessary for performing their tasks.

Manual records are kept in locked archives, accessible only to individuals authorized according to confidentiality regulations.

Electronically stored data is protected by electronic access rights. The supervisor determines individual access rights for staff based on their job responsibilities.

Software applications have personal user accounts, as well as access to workstations. The use of information systems and the data within them is monitored on a user-specific basis.
RIGHT TO INSPECTION

The patient has the right to know, without being hindered by confidentiality regulations, what information about them is stored in the personal data register (Patient Act, Sections 26-28).

The right of a minor to access information about themselves is determined according to general provisions on their legal capacity.

Authorities have the right to access information from the register in accordance with the Act on the Openness of Government Activities (Sections 6.4.2 and 6.4.3). The right to inspection can only be denied in exceptional cases. Denial may be based on grounds such as the potential serious harm to the patient's health or treatment, or the rights of others.

A request for inspection can be made in person, with a handwritten signature, or electronically (in a reliable manner).

The patient has the right to review and view their own patient records and, upon request, receive them in writing.

The identity of the person exercising the right to inspection shall be verified.

The use of the right to inspection is free of charge once a year.

The requested information must be provided for inspection no later than one month after the request is made.

RIGHT TO REQUEST CORRECTION OF INFORMATION

If the data subject discovers incorrect or incomplete information about themselves, they can request the correction of the information within one month of discovering the error. The request for correction should always be made either:

a) Electronically: info@cityklinikka.fi
b) In writing: Cityklinikka, Aleksanterinkatu 21 A, 00100 HELSINKI

The identity of the data subject will be verified before any further action is taken.

The decision regarding the correction of information is made by the treating physician or the most recent attending physician. If the patient's request is justified, the correction is made by a person who has specific authorization to correct patient record information.

Any erroneous entries are crossed out or moved to a background file in a way that both the erroneous and corrected entries can be read later. The name, position, and date of the person making the correction must be indicated in the patient records. (Decree of the Ministry of Social Affairs and Health on the Preparation of Patient Records 298/2009)

Patient register information is confidential. The data subject does not need to explicitly state a prohibition on the disclosure of information. According to Section 30 of the Health Care Act, "the data subject has the right to prohibit the controller from processing information concerning him or her for direct advertising, distance selling, and other direct marketing as well as for market and opinion research."

The patient/customer/legal representative may withdraw their consent at any time.

STORAGE, ARCHIVING AND DISPOSAL

Patient information is stored in accordance with the decree 298/2009 of the Ministry of Social Affairs and Health. Patient records are disposed of in a manner that prevents unauthorized access to the information by third parties.

Electronic inquiries and image consultation requests received through the website are deleted one year after the customer's contact, if no customer relationship has been established. If an inquiry or consultation request leads to a customer relationship, the requests are stored and disposed of in accordance with the decree 298/2009 of the Ministry of Social Affairs and Health.

OTHER

During the implementation of the software, the staff has received training and instructions. IT support personnel and administrators have received more comprehensive training. Training and guidance for new staff members are provided through an orientation program. The CEO is responsible for the functionality and technical security of the information system.

The staff members sign a confidentiality agreement upon entering into an employment contract.