

Privacy Policy

On data processing related to medical treatment

Swiss Medical Services Egészségügyi Korlátolt Felelősségű Társaság (seat: ground floor 4, 22 Kinizsi utca Budapest, Hungary, H-1092; company registry number: 01-09-561648, tax number: 12171864-2-43), as data controller hereby publishes its policy regarding its data processing activity in connection with medical treatment and the related services. Natural persons ('data subjects') can access this Privacy Policy on the website of the data controller, and on the service locations listed in section 6.1.

1. Interpretative provisions

- 1.1. For the purposes of this Privacy Policy, medical treatment shall be any activity related to the direct examination, treatment and medical rehabilitation of the data subject, and for that purpose, the processing of the examination materials of the data subject, including the provision of medicines, medical tools, medical care, rescue and patient transportation and obstetric care, performed for the preservation of health and for the prevention, detection, early diagnosis and curing of illnesses, improving or maintaining the condition resulting from the illness.
- 1.2. For the purposes of this Privacy Policy, medical data is any data related to the bodily, mental and psychological condition, pathological passions and the circumstances of the illness or death of the natural person as the data subject, the cause of death, as reported by him or her or by any other person about him or her or any data resulting from tests, measurements, imaging or any derived data recorded by the health care network; and any data affecting the abovementioned details (e.g. behaviour, environment, occupation).
- 1.3. The terms "personal data", "data controller", "data processing", "personal data breach", "supervisory authority" and "third party" are used in their meaning defined in Article 4 of the General Data Protection Regulation referred to in section 1.4, and shall be interpreted accordingly.
- 1.4. "General Data Protection Regulation": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (General Data Protection Regulation, hereinafter referred to as "GDPR").

2. The legal basis for the processing of personal data

- 2.1. If the data processing is performed in connection with the performance of the contract between the data subject's employer and the data controller, the legal basis for data processing is the performance of the existing contract between the data controller and the employer pursuant to Article 6 (1) (b) of the General Data Protection Regulation, in accordance with Section 58 (1) of Act XCIII of 1993 on Occupational Safety.
- 2.2. If the data is processed in connection with the performance of a contract between the natural person as the data subject and the data controller, the legal basis for data processing is the performance of the relevant contract between the parties under Article 6 (1) (b) of the General Data Protection Regulation.
- 2.3. If a natural person uses the health care services of the data controller as a data subject funded by the National Health Insurance Fund Manager then, according to Article 6 (1) (e) of the General Data Protection Regulation, data processing is necessary for the performance of a task in

the public interest or for the exercising of public powers delegated to the data controller.

2.4. Regarding contact details, the legal basis for data processing is the consent of the natural person ('data subject') in line with Article 6 (1) (a) of the General Data Protection Regulation.

3. The subjects of data processing

3.1. In the case of data processing defined in section 2.1, data subjects of the data processing are natural persons who are in employment or any other legal form of working relationship with the employer.

3.2. In the case of data processing defined in section 2.2, data subjects are natural persons who are in a contractual relationship with the data controller.

4. **The processed data, purpose and period of data processing**

The processed personal data	Purpose of data processing	Period of data processing
<i>Personal data</i>		
Identification data (name, place and date of birth, mother's birth name)	Identification of the natural person ('data subject')	For at least 30 years from the date of recording as part of the medical documentation; for at least 50 years as part of the final report
Social security number	Financing the care at the National Health Insurance Fund Manager, identification of the data subject as natural person	For at least 30 years from the date of recording as part of the medical documentation; for at least 50 years as part of the final report
Address	Communication with the data subject	For at least 30 years from the date of recording as part of the medical documentation; for at least 50 years as part of the final report
Phone number, email address	Communication with the data subject (optional)	Until the consent of the data subject is withdrawn or the purpose of data processing is terminated
<i>Special category personal information</i>		
Medical data provided by the data subject	Records of previous known diseases and factors affecting occupational health	For at least 30 years from the date of recording as part of the medical documentation; for at least 50 years as part of the final report
Medical data collected by a data controller	Assessment of the working capacity of the employee	For at least 30 years from the date of recording as part of the medical documentation; for at least 50 years as part of the final report

5. **Additional provisions for the period of data processing**

5.1. The medical records must be kept for at least 30 years from the date of the data collection, and

the final report for at least 50 years. If justified for medical or scientific research purposes the data may be stored after the expiry of the mandatory retention period; if further storage is not justified, the records should be destroyed.

5.2. Records created by imaging diagnostic methods (X-ray, CT, etc.) shall be retained for a period of 10 years from the date of their creation, whereas the examination result prepared based on the records shall be retained for 30 years from the date of the creation of the records.

6. Storage and security of personal data

6.1. If the records are stored in printed form, the data controller shall store the medical records of the data subjects in lockable cabinets located at the premises of the data controller in accordance with Appendix 1. The storage shall be reviewed every three months.

6.2. The storage location of the printed documents depends primarily on the outpatient clinic that the data subject visits to use the occupational health services provided by the data controller. In this case, the medical records are typically stored at the location provided by the employer. If the service was used several years earlier, the data controller archives the documents containing the data, and stores it in a locked filing cabinet leased from the data processor, as per section 7.1.4.

6.3. The electronically recorded medical records are stored on limited access servers located in facilities supervised by the data controller: partly on controller's own servers and partly on leased servers. A data processor is involved in the storage of the data as described in section 7.1.5. When transmitting medical data on the open public network of the Internet, data protection is ensured by SSL (Secure Socket Layer) protocol-based encryption.

6.4. The data controller uses the EKarton2 patient management system developed by itself, and the Europroof resource planning system to record personal and medical data in such a way which facilitates the administration of the treatment for the physicians and natural persons involved.

7. Use of data processors

7.1. For the purposes of the treatment, the data controller involves the following data processors in the data processing:

7.1.1. In case of an occupational health examination: Genova Diagnosztika Magyarország Kft. (seat: 6/b Tállya utca H-1121, Hungary; tax number: 25378102-2-43);

Genova Labor Hungary Kft. (seat: 6/b Tállya utca H-1121, Hungary; tax number 25378119-2-43);

7.1.2. If imaging diagnostic procedures are necessary: B.Radiológiai Centrum Kft. (seat: 8-14 Nagyenyed utca, Budapest, Hungary H-1123; tax number: 24725446-2-43; e-mail: info@budairc.hu);

7.1.3. In case of laboratory testing: In case of laboratory testing: Centrum-Lab Kft. (seat: 1-5 Lövház utca, Budapest, Hungary, H-1024; tax number: 14735451-2-41; e-mail: info@centrumlab.hu);

Synlab Hungary Kft. (seat: Floor 1, 53 Bajcsy-Zsilinszky út, Budapest, Hungary, H-1065; tax no.: 14872925-2-42, e-mail elérhetősége: hungary@synlab.com);

7.1.4. For other non-occupational health examinations: Swiss Medical Hungary Zrt. (seat: 15/b Táltos utca, Budapest, Hungary, H-1123, ; tax number: 22989143-2-43; e-mail address: info@swissclinic.hu);

7.1.5. Regarding document storage: Illés Logistics Zrt. (seat: (2611/1 Százhalombatta, Hungary, H-2440; tax number: 23341779-2-13);

7.1.6. For electronic storage: DEEPBLUE System Ltd. (seat: 16 Márvány utca, Budapest

Hungary, H-1012; tax number: 13810380-2-41; e-mail address: info@deepblue.hu;

7.1.7. Finally, the doctors participating in the treatment are involved as data processors, as specified in Appendix 2, reviewed every three months.

7.2. The data controller reserves the right to involve further data processors in the processing in the future, which will be communicated to the data subjects by amending this Privacy Policy.

8. The persons authorized to access the data and the conditions of any transfer

8.1. Only the data controller and natural persons in the employment of or other legal form of working relationship with the data controller, and involved in medical treatment are entitled to access the data.

8.2. Data transfer is possible only if it is required by the law; the data controller can transfer the personal data in his possession to governmental agencies only in exceptional cases. These include the case when the data subject is suffering from a serious infectious disease for which epidemiological rules require the notification of appropriate health care facilities (e.g. the National Public Health and Medical Officer Service, the National Center for Epidemiology).

9. Rights of data subjects in relation to data processing

9.1. Information on the data processing by the data controller can be requested from the data controller's data protection officer.

Name of data protection officer: Béla Droppa

Postal address: 67. Vörösmarty utca Budapest, Hungary H-1064

Phone: +36 1 605 0302

E-mail: dpo@swissclinic.hu

9.2. The data subject may request information in writing from the data controller on the contact details defined in section 6.1 on the personal and medical health data managed by the data controller, and may request the indication, purpose and source of the legal basis, and the period of the data processing; and may also request information on when, to whom, and by what authorization the data controller provided access to or transferred his or her personal or medical data.

9.3. The data subject has the right to object to the processing of his/her personal data contained in the health documentation, to have access to his/her medical records and to have the right to be informed of his/her health data provided that the health records shall be controlled by the data controller as a health care provider and the data contained therein shall be controlled by the patient as the data subject.

9.4. Furthermore, the data subject has the right to

9.4.1. access the health documentation, and to make an extract or a copy of it;

9.4.2. receive an outpatient care sheet upon completion of the outpatient care;

9.4.3. obtain a summary or an excerpt of the medical opinion on his or her medical data.

9.5. The data is not automatically processed, so the right to data transfer is not applicable for the data processing.

9.6. No automated decision-making occurs.

10. Limitations and special cases of the right to access

10.1. Where the medical records of the data subject also contain data relating to the rights of another person to private data, the data subject may exercise his/her right of access only in respect of the

part concerning himself or herself.

- 10.2. Only a person defined in Act CLIV of 1997 on Health Care may have the right to access the documentation of an incapacitated patient.
- 10.3. On the basis of a written request from the spouse, immediate relative, brother, and partner of the data subject, the data controller shall grant access right to the health records if the conditions specified in the law are met;
 - 10.3.1. the medical data is required for the purpose of diagnosing a cause affecting the life, health of the applicants, or their medical care; and
 - 10.3.2. it is not possible to directly or indirectly learn the health data in any other way.
- 10.4. Upon the death of the data subject, his/her legal representative, close relative and heir shall be entitled, on the basis of his/her written request, to obtain medical information related to the cause of the death, to the medical treatment prior to the occurrence of death, to access the health documentation and to make extracts and copies thereof at his or her own expense.

11. Medical Confidentiality

- 11.1. The persons participating in the medical treatment may disclose the medical secrets – which are a set of medical and personal data – only to those having access rights to them, and to treat them as confidential.
- 11.2. The data subject has the right to declare which natural persons may be informed of his or her illness and its expected outcome, and which natural persons are excluded from gaining partial or complete information of his or her medical data.
- 11.3. The data controller provides enhanced protection for the medical secrets he has become aware of; he is entitled to release the medical secrets to a third party only if the data subject, in full knowledge of the scope of confidential data to be disclosed, grants his or her consent to the disclosure of the data or if the data controller is authorized or obliged to disclose the data by the law.
- 11.4. The health data of the data subject shall be disclosed in the absence of his or her consent, if
 - 11.4.1. it is required by law;
 - 11.4.2. it is necessary for the protection of the lives and health of others;
 - 11.4.3. a person caring for the data subject may be provided with the medical data which, if they remain unknown, may lead to a deterioration of the data subject's health.

12. Remedy options available for the data subject

- 12.1. Complaints can be made on the activities of the data controller and a procedure of the data protection authority can be initiated under section 52 of Act CXII of 2011 at the Supervisory Authority.

Name: Hungarian National Authority for Data Protection and Freedom of Information (NAIH)

Seat: 22/c Szilágyi Erzsébet fasor, Budapest, Hungary, H-1125

Postal address: Pf. 834, Budapest, Hungary, H-1534 (PO Box)

Phone: +36 (1) 391-1400

Telefax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu

- 12.2. In case of violation of his/her rights, the data subject apply to a court against the data controller. A civil lawsuit shall be initiated at the Regional Court of Budapest. The lawsuit may – at

the discretion of the data subject – be initiated also before the regional court with jurisdiction at permanent or temporary residence of the data subject (the contact details and list of regional courts can be found on the following link: <http://birosag.hu/torvenyszekek>).

In matters not covered by this privacy policy, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data, Act CLIV on Health, Government Decree 89 of 1995 (VII. 1.4) on the Occupational Health Service and the Classification of Employees by Categories, Act XCIII of 1993 on Work Safety, and Act CXII of 2011 the Right of Informational Self-Determination and Freedom of Information shall govern.

In addition, the data controller undertakes to act in accordance with the relevant contract executed with the data subject or his or her employer, the applicable rules and the legal practice in the course of its data processing activities and in exercising its confidentiality obligations, and to comply with the provisions of applicable law.

Date: Budapest, 25 May 2018.