Sanacare AG
Schützenstrasse 1
8401 Winterthur

+41 52 264 04 60
datenschutz@sanacare.ch
www.sanacare.ch

DATA PROTECTION DECLARATION FOR OUR PATIENTS OF THE COMPANY HEALTH SERVICES (MEDICAL CENTER)

Version from 03.09.2024

Dear Patient

This privacy statement refers to the requirements of the applicable Swiss Data Protection Act ("DSG" or "revDSG") incl. the applicable Ordinance on Data Protection ("VDSG" or "DSV") as well as the EU General Data Protection Regulation ("GDPR"), where relevant. Whether and to what extent these regulations are applicable, however, depends on the individual case.

Below, we explain the processing of your data from a data protection perspective and inform you about your rights, which you can exercise within the framework of data protection.

The term "data" refers to personal data (health data, administrative data). "Processing" means any handling of your data (recording, changing, sharing, storing, deleting, etc.).

Responsibilities

Sanacare AG is responsible for the data processing described in this privacy policy. Your health data is primarily processed by the employees of our Medical Centers at the company locations. Therefore, if you have any questions regarding the content of your patient file or if you would like a copy of your file, please contact your responsible Medical Center directly. If you have any questions about data protection or if you wish to exercise your rights under data protection, please contact our data protection officer in writing using the following contact details:

Sanacare AG
Data Protection Officer
Schützenstrasse 1
8401 Winterthur
datenschutz@sanacare.ch

We provide our services (Sanacare AG) on behalf of your employer. Unless you have given your explicit consent, the employer has no right to view your data. As an order processor, Sanacare AG is responsible for complying with the contractually agreed and legally prescribed requirements.

Collection and purpose of data processing

The collection, storage, processing, use and retention of your data is based on legal requirements and the treatment contract and serves to document and fulfil the purpose of the treatment. The collection of data is carried out by the attending physician. There may also be other health professionals, who provide us with medical records about your current or past treatments after you had given your consent.

Only data related to the provision of services contractually agreed on with your employer will be processed in your patient file. The patient file includes the personal information provided on the patient form, such as personal details and contact data, as well as health data collected during the provision of services, such as medical histories, diagnoses, therapy proposals and findings, and other health data necessary for the fulfilment of the contractual agreements. Furthermore, your file may also

contain documents from external health professionals and institutions, insurance companies, authorities and official bodies. The services resulting from the treatment are also recorded in your patient file.

Access to data and confidentiality

In our system for maintaining patient records, access to your data by authorised health professionals (doctors and medical staff of the Medical Center) only takes place within the framework of the above-mentioned service provision. In the context of certification and review procedures, we must also grant access to personal data to the responsible companies and persons such as auditors and inspectors, which may include your data. All persons authorised to access the data are obliged to maintain confidentiality.

Disclosure of data

We only transfer or disclose your personal data, in particular medical data, to external third parties if it is permitted or required by law or if you consent to the disclosure within the framework of our service provision, including treatment.

Recipients of your personal data may include:

- Further-treating physicians or laboratories: in individual cases (after your consent)
- HSE responsible persons (or occupational safety): for accident reporting in the case of an accident or for pregnancy-related workplace risk analysis (after your consent).
- Accident or disability insurance: for assessment of insurance benefits (according to ance with legal provisions)
- Your employer: Occupational health assessment results will only be communicated as simple conclusions (suitable, conditionally suitable, not suitable, etc.) at end of your consultation as a filled-out form that you can handover to your employer. In individual cases, data related to workplace risk analysis or reintegration (case management) may be transferred (after your consent). In addition, contractually agreed data, e.g. anonymised statistics, may disclosed.
- SUVA: results of the preventive medical exams (in accordance with legal provisions)
- Authorities: Conclusions of compulsory heath examinations, (e.g. SECO exams, may also be disclosed to the responsible authorities, e.g. SECO. The underlying documentation (including your medical records) is not included in the transmitted documents (e.g. in the filled-out form). The data may only be transmitted upon a specific request of the law enforcement nt and supervisory authorities.
- Representatives of the pension fund: for verification of benefits in individual cases after your consent)
- Future service providers: If your employer changes to another medical service provider, the existing data will be transferred to the future service provider to ensure treatment continuity. The transfer is made through channels that are not accessible to your employer. The subsequent service provider will a be a subject to the same confidentiality and data protection obligations as Sanacare AG.
- As part of the Novartis Executive Check-Up Program, administrative data is transmitted to the Novartis Medical & Security Risk Provider. This is for the purpose of billing services and recording the number of examinations and referrals to external service providers.

Communication

In order to communicate with you and third parties and to exchange data, we use various means and channels of communication, such as telephone, mobile phone, SMS, letter post or email. Since personal data is considered as particularly sensitive, we place a high value on the security of communication. Various technical and organisational measures are implemented to protect your data and maintain confidentiality. For example, the Medical Center only sends your data via secure communication channels, in particular emails only encrypted (HIN). When communicating by SMS, please note that depending on the registration, the message may appear on several mobile devices at the same time (e.g. a mobile phone and a tablet). If these devices are used by other users such as family members, the messages may be read. If you have communication preferences or wish that some means of communication should be avoided, , please inform your responsible Medical Center.

Your rights

Withdrawal of your consent

If you have given your consent for data processing, you can withdraw it at any time in the future. The revocation of consent must be made in writing. The legitimacy of the data processing carried out until the revocation date remains unaffected by the revocation.

Inquiry-, access and issuance requests

You have the right to obtain information about the collection, recipients and purpose of the processing of your personal data free of charge at any time. Furthermore, you have the right to review and/or receive a copy of your patient file free of charge.
To make use of your right to information, please contact your responsible Medical Center. For data protection reasons, you will be required to show a valid photo ID or passport. This also applies to legal representatives and/or authorised persons, who in addition need to present the power of attorney. After your identity verification is completed, a copy of your patient file will be prepared and can either be handed over to you in person at the Medical Center or sent to you by mail.

Correction of information

If you discover or believe that your original or processed data is incorrect or incomplete, please report this to your Medical Center. We will investigate your request for rectification and, if applicable, implement it accordingly.

Statutory Retention and deletion

As legally required and for the purpose of exercise, defence or assertion of legal claims a copy of your data will be kept within the limitation periods for 40 years after termination of the contractual agreement with your employer or from the last treatment entry. Your patient file will be irrevocably deleted after expiration of the legally prescribed retention obligation or after expiration of the limitation period.

Data Protection

We take appropriate security measures to maintain the confidentiality, integrity and availability of your data and to protect it against unauthorised or unlawful processing as well as against the risks of loss, accidental alteration, unauthorised disclosure or access. Security measures may include, for example, measures such as the encryption and pseudonymisation of data, logging, access restrictions, the storage of security copies, instructions to our employees, confidentiality agreements, access and access controls, personal data carrier controls, authentication of authorised persons, disclosure and storage controls. Where third parties process your data on our behalf, we oblige them to take appropriate security measures.