

## **Data Protection – We Respect your Rights to Privacy**

Any data relating to your person including health care services are governed by the Data Protection Bill and are dealt with in compliance with the directives of the General Data Protection Regulation. Making it easy for you to assess which professionals respectively institutions in the public health sector are involved in medical care procedures performed in our hospital, we prepared a list of information specified below:

### **Processing of personal data for one or more specified purposes:**

In line with your medical treatment data relating to your person, including your social status, medical data necessary for your treatment are collected, recorded, saved, processed, retrieved, employed, transferred, etc. Overall, the reference here is processing of your personal data. The term “processing” constitutes the generic term with all the activities specified above. The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if there is a valid consent of the patient in place.

Treatment-related procedures require particularly processing of your personal data for the purposes of preventive medicine, including medical diagnosis, medical treatments, benefits of cure and medical aftercare. Data processing – in terms of best possible medical care - is also necessary for interdisciplinary team conferences to analyze and discuss diagnostic procedures and treatments, including pretreatment, co-treatment and further therapies regarding diagnostic management, treatments, diagnostic findings and health & vital status. In addition, doctor’s reports and medical reports are written and processing of personal data is performed to ensure quality assurance, including identification and combat of hospital-acquired infections, as well as for the provision of pastoral service and social care and for the hospital discharge management.

Secondary to processing of your personal data necessary for providing medical care services, administrative management is further required in your medical treatment. This basically involves processing of your personal data for medical billing purposes relating to your medical treatment, including controlling purposes, invoice verification, enforcement of claims, exercise or defence of legal claims, etc. In addition, processing is necessary for purposes of academic training, including further training and continuing education of physicians and staff members of other health-care professionals, scientific research purposes or legal obligation to register (for instance obligation to register with the police according to the notification order, to the public health department complying with the infection protection law, and the Bavarian Cancer Registry), and last but not least for reasons of support service and maintenance of IT systems and computer applications, etc.

### **From which parties do we collect your personal data?**

Whenever possible, we fundamentally collect relevant data from you personally. In some cases, it may occur that we receive person-related data and information relating to your person from other hospitals, which performed primary care or preoperative care, including office-based physicians, medical specialists, medical care centers (so-called MMC), etc. Such data are consolidated in our facility in terms of a standardized case documentation with your other data.

### **Who has access to your data?**

Persons involved in the medical care or treatment provided to you have access to your data, and this also includes physicians from other departments providing multidisciplinary co-treatment or staff members of the administration division in charge of preparing medical billing covering medical treatments. Your data are processed by professionals or assisting professionals working under their responsibility. These professionals are bound by professional secrecy obligation or subject to general duty of confidentiality.

We provide appropriate safeguards for the fundamental rights and interests of the data subject!

## **Legal basis for processing your data by the hospital owner**

The legal basis for permitting hospital owners to process your personal data in compliance with data protection regulations arises from the fact that the hospital owner is the responsible body in providing health care and medical treatments in patients. On this basis, there are various laws and regulations applicable in compliance to which the hospital owner has permission for processing your personal data.

The European General Data Protection Regulation (EU GDPR) in particular shall be mentioned, for instance Art. 6 and Art. 9, GDPR, which are equally applicable to German Law expressly regulating that personal data of patients may be processed. In addition, there are fundamental principles laid down in the German Law, for instance Fifth Book of the Social Code (SGB V), for example paragraph 301 SGB V, and paragraph 630 BGB (German Basic Law), with the assumption is made that processing of personal data is necessary.

The legal basis for processing your data include following examples:

- Processing of data for the purposes of clinical management of a patient including inter-disciplinary and inter-professional communication on the patient for treatments (Art. 9 section 2h, section 3, section 4 GDPR in connection with paragraph 630a ff, 630f BGB (German Basic Law) in connection with relevant provisions of federal state law, if there are any).
- Data transfer to “third parties” in terms of co-treatments (by means of a multi-disciplinary team), external consultations with medical specialists, for instance assessment of diagnostically relevant laboratory findings, telemedical procedures, including consultation with third-party therapists (Art. 9, section 2h, section 3, section 4 GDPR in connection with Art. 27 BayKrG (Local Hospital Law of the Free State of Bavaria),
- Data transfer to statutory health insurance companies for the purpose of settlement of medical bills (Art. 9, section 2h, section 3, section 4 GDPR in connection with paragraph 301 SGB V),
- Data transfer for the purpose of quality assurance (Art. 9, section 2i GDPR in connection with paragraph 299 SGB V in connection with paragraph 136 SGB V respectively directives of G-BA) (The paramount decision-making body of the self-government is the Federal Joint Committee (G-BA), etc.

In addition to this, personal data may be processed in those cases for which there is your valid consent in place.

## **Why we need you to give us your personal data**

It is necessary that you share your personal data with us for proper administrative management of medical treatment services provided by us. This excludes only cases involving anonymous birth.

## **Whom do we share your personal data with?**

Your personal data are collected and processed for the purposes identified in full compliance with Data Protection Law respectively optional valid consent in place, and such personal data are shared with third parties, when appropriate. Third parties concerned we may share your personal data with include in detail:

- Statutory health insurance companies, in case you are covered under a statutory health care plan,
- Private health care insurance, in case you are covered under a private health care program,
- Accident insurance providers,
- General practitioners,
- Physicians providing further treatment, including providing postoperative treatment and aftercare respectively physicians providing co-treatment,

- Other facilities in the health care system or other medical treatment providers,
- Rehabilitation hospitals,
- Care providers,
- Third party data processors (so-called data processing companies, for instance companies providing private medical billing services, IT service providers) including
- Pastoral service providers

### **Which specific personal data are transferred?**

In every individual case, it very much depends on the data receiver and the predetermination for specific purposes, which personal data are transferred. Personal data for transfer to your health insurance provider is in full compliance with paragraph 301 SGB V and includes the following details:

1. Name of the insured person,
2. Date of birth,
3. Address,
4. Health insurance policy number,
5. Policy holder type,
6. Date, time and reason for hospital admission, including referral diagnosis, admission diagnosis, and when there is a change in admission diagnosis, additional diagnoses are mentioned, estimated hospital stay, and in case of extended length of stay making an explanatory medical statement to the health insurance company upon their request, and for infants up to one year weight on admission shall be stated.
7. Date and time of surgeries and other procedures performed in our hospital,
8. Date, time and reason for hospital discharge respectively reason for transfer to another health care facility, including main diagnosis and secondary diagnoses relevant in leading to inpatient treatment.
9. Detailed information on rehabilitation procedures performed during inpatient treatment, including information to fitness for work and recommendations regarding type of further treatment indicating adequate facilities for aftercare.

### **Medical treatment for aesthetic surgeries, tattoos or piercings**

In the case, that there is a condition, which is suspicious to be the consequence of aesthetic surgeries, tattoos or piercings and without indication for medical intervention, relevant information shall be sent to your health insurance company.

### **Right to withdraw your consents granted at any time**

You have the right to withdraw your consent at any time, when the consent you granted the hospital owner involves the use, disclosing and processing of your personal data. You have the option to send us your withdrawal of consent notice in written form / by e-mail / by fax. There is no need for indicating any reasons. Your withdrawal of consent will take effect upon receipt of your withdrawal of consent notice. It has no retroactive effect. Up to this effective date, using, disclosing and processing of your personal data remains lawful.

### **Safeguarding of legitimate interests of Klinikum Nürnberg**

In the case that medical bills prepared by Klinikum Nürnberg remain unsettled, Klinikum Nürnberg shall seek professional legal assistance and assert their claims in court against you or your health insurance company, and Klinikum Nürnberg (for the purpose of asserting our legal rights) has the right to disclose your personal data and data relating to your medical treatment.

## **How long will your personal data be stored?**

In compliance with paragraph 630f BGB (German Civil Code) Klinikum Nürnberg is legally obligated to keep effective patient care documentation relating to your medical treatment. This obligation can be met in hardcopy form or as electronic patient record. This patient record documentation will be retained for a long time even after finishing of your medical treatment. We are required by law to follow such procedure.

A number of specific governing-law provisions provide definition how long medical records in detail must be retained by the hospital. Notable examples to be mentioned are paragraph 630f BGB (German Civil Code), Ordinance On The Protection Against Dangers Arising From X-rays (RöV), Radiation Protection Act (StrlSchV), Ordinance On The Operation Of Pharmacies (ApBetrO), Transfusion Law (TFG), and many more. These governing-law provisions regulate different compulsory periods of record-keeping.

In addition, it must be observed that hospitals are allowed to retain patients' medical records up to 30 years for purposes of preservation of evidence.

For this reason, your patient medical record will be retained for up to 30 years.

## **Right of access to personal data, to information, rectification, erasure, etc.**

You are entitled to specific rights, meaning exercising rights as person affected in each individual case. You may exercise these rights towards the hospital owner. These rights are set out in the EU General Data Protection Regulation (GDPR) and are also in force in Germany:

### - Right of access and information, Art. 15 GDPR

You shall have the right of access and information to personal data which have been collected concerning you.

### - Right to rectification, Art. 16 GDPR

You shall have the right to obtain without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

### - Right to erasure, Art. 17 GDPR

You shall have the right to obtain the erasure of personal data concerning you when there are specific reasons for erasure of personal data. This is particularly the case when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

### - Right to restriction of processing, Art. 18 GDPR

You shall have the right to obtain restriction of processing of personal data. This means that your personal data are not erased but rather clearly marked and put on a suppression list for restriction of further processing or use.

### - Right to object to unacceptable processing of your personal data, Art. 21 GDPR

In principle, you have a general right of objection even to legitimate processing of personal data, which are necessary for the performance of a task carried out for reasons of public interest, for the exercise of official authority or legitimate interest of the establishment.

## **Right to lodge a complaint with a supervisory authority for privacy breach**

Without prejudice to any other administrative or judicial remedy, you shall have the right to lodge a complaint with a supervisory authority, of the alleged infringement if you consider that the processing of personal data relating to you infringes this Regulation. This is pursuant to Art. 77 GDPR. You may lodge your complaint in writing with

Bayerische Landesbeauftragte für den Datenschutz, Postfach 22 12 19, 80502 München.

## **Data protection officer in charge at Klinikum Nürnberg**

Klinikum Nürnberg appointed their data protection officer. His contact details are:

[datenschutz@klinikum-nuernberg.de](mailto:datenschutz@klinikum-nuernberg.de)

Please do not hesitate to contact his office.