PRIVACY POLICY ON ELECTRONIC HEALTH DOSSIER (DSE)

Pursuant to the General Data Protection Regulation (EU Regulation 2016/679) and Legislative Decree 196/2003 s.m.i.

INTRODUCTION

The Fondazione IRCCS - Istituto Nazionale dei Tumori di Milano (hereinafter referred to as the "Foundation") informs you of the processing of the personal data that you will provide us with in order to allow you to consciously express your consent to their processing by means of the electronic health record electronic health record (DSE) of the Nuova Piattaforma Informatica Regionale di Integrazione ("NPRI").
The DSE is made up of the set of personal data generated by present and past clinical events at the Foundation and constitutes a specific personal data processing.
In particular, the DSE is made up of the set of health data in electronic format relating to your state of health, collected during present and past clinical events (e.g. reports of outpatient visits, hospital discharge letters, etc.) relating to services carried out both under the institutional and freelance regimes.
The subjects who will process your personal data have been formally authorised to manage the information concerning you as provided for by the regulations in force.
It should also be noted that the health data collected through the health record may be processed, like any other clinical information, also for research purposes in compliance with the provisions of the sector regulations.

DATA CONTROLLER

The data controller is:
Fondazione IRCCS Istituto Nazionale dei Tumori
Via G. Venezian, 1 - 20133 Milano
Ownership of the processing is exercised by the Director General
e-mail: direttore.generale@istitutotumori.mi.it
Delegated for processing are the Medical Directors of the Foundation's Operating Structures where processing is carried out.

DATA PROTECTION OFFICER

The Data Protection Officer can be contacted at the following addresses::

- e-mail: DPO@istitutotumori.mi.it
- PEC: formazione.privacy@pec.istitutotumori.mi.it

DATA PROCESSOR

The data controller, Aria S.p.A., appointed by the Foundation as provided for by art. 28 of the GDPR, avails itself of the support of external companies, appointed as sub-processors as provided for by art. 28 co.4 of the GDPR, for the management and maintenance activities of the applications. Your personal data may therefore be processed by the personnel of the company supplying the application and the NPRI cloud computing service module DSE, only because of assistance or technical support activities, or in the event of exercising the right of access for data extraction activities.

MODALITY

The Foundation processes **personal data and special categories of data** (including health-related data) electronically.

PURPOSE

Data processing through the use of the DSE is aimed at **improving your care process** through integrated access to your information by the healthcare professionals involved. In this way, the professionals involved in your clinical pathway can have timely access to all the clinical information acquired at the Foundation, regardless of the department that generated it.
The Foundation may process the data on your DSE for purposes of study and **scientific research** in the medical, biomedical and epidemiological fields.

LEGAL BASIS

The DSE can only be established with **your free and optional consent**. Please note that, in the event of refusal, you will still be guaranteed to receive the requested medical treatment and your data will only remain available to the health professional who compiled them, without their inclusion in such an instrument.

SUBJECTS AUTHORISED TO PROCESS

The data will be processed by **authorised and duly designated personnel** of the Foundation, in compliance with the obligations of confidentiality and protection of the dignity and integrity of the persons concerned. It is emphasised that the authorised personnel of the Foundation are subject to professional secrecy, i.e., official secrecy.
The Foundation guarantees **compliance with the technical and organisational security measures** for the protection of data provided for by the relevant legislation in force.
Consultation of the data necessary to achieve the purposes envisaged by the DSE **is permitted**

- to the healthcare professionals of the Foundation who will provide healthcare assistance over time and in various capacities, both under the NHS and under the intramoenia (intramoenia) freelance healthcare scheme
- to researchers for the time necessary for the specific research study,
- to staff performing administrative functions closely connected with the patient care pathway,
- to healthcare personnel fulfilling reporting obligations due to the Ministry, the Region and the ATS.

Access to the DSE will be limited to personnel involved in the treatment process and **will NOT be allowed**

- to operators of other Health Authorities,
- your General Practitioner (GP) or Free Choice Paediatrician (PLS),
- experts, insurance companies, employers,
- scientific associations or organisations,
- administrative bodies also operating in the health sector,
- medical personnel in the exercise of medico-legal activities.

Authorised parties access the DSE by means of authentication procedures that make it possible to trace the identity of the professional and the actions performed. In any case, your personal data contained in the DSE will not be disseminated.

DATA RETENTION

L'indice dei dati e documenti del Suo DSE è cancellato dal titolare del trattamento decorsi trenta (30) anni dalla data di istituzione, con periodicità annuale. Al termine del periodo di conservazione, per mantenere attivo il Suo DSE per le finalità previste, le verrà chiesto di esprimere un nuovo consenso al trattamento.

RIGHTS

You may at any time exercise, within the limits and under the conditions laid down in Articles 15-22 GDPR, the right to access, rectification, portability, deletion of data, restriction and opposition to processing. You are also reminded that, for the processing of personal data based on the data subject's consent, you have the right to withdraw your consent to the processing of personal data at any time, where expressed, without prejudice to the lawfulness of the processing based on the consent given before the revocation.
These rights may be exercised by contacting the Data Controller at the following addresses:

Ufficio Relazioni con il Pubblico
E-mail: urp@istitutotumori.mi.it | Telefono: 02 2390 2772 | Fax: 02 2390 3316

o Withdrawal of **consent**
You have the right to revoke your consent to the processing of your data in writing at any time. The processing of your data carried out before revocation remains lawful. In the event of withdrawal of consent (freely given at any time), the health record will not be implemented any further.
o **Right to obscuration and de-obscuration**
You may request that individual clinical events concerning you be obscured, i.e. you may decide not to have all or some of the information relating to the clinical event concerning you included in your DSE. Obfuscation of the clinical event is carried out in a technical manner that ensures that those authorised to consult your DSE can neither view the obscured event, nor become aware that you have made this choice. With the obscuration procedure, the obscured reports/episodes will no longer be available for consultation through the Health Record tool and, therefore, clinicians will not be able to view the obscured data, even in an emergency/urgency. The obscured data or individual episode will remain visible only to the professional who provided the obscured service.
The right to blackout may be exercised

- during check-in at the **CUP**;
- by notifying the **referring doctor** of your wish to have your data blacked out;
- at a **later stage**, by contacting the Privacy Function and DPO.

Conversely, at any time you may request that the visibility of previously obscured episodes be restored**(de-dimming**).

CLAIM TO THE AUTHORITY

Pursuant to Article 77 of the Regulation, if you consider that the processing of your personal data violates the legislation on the protection of personal data, you have the right to lodge a complaint with the Italian Data Protection Authority or with the supervisory authority of the EU Member State in which you habitually reside or work or in the place where the alleged violation occurred.

THE ELECTRONIC HEALTH RECORD (DSE)

FAQ | GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1 WHAT IS THE HEALTH RECORD?

The health record is the set of personal data generated by present and past clinical events concerning the person concerned, which are shared between the health professionals who care for him/her at a single health facility (e.g. hospital, private nursing home, etc.).

2 WHAT IS THE HEALTH RECORD FOR?

The health dossier serves to make the processes of diagnosis and patient care more efficient within a single health facility, allowing the various professionals working there to access all the clinical information relating to the patient's previous interventions (admissions, outpatient visits, emergency room visits) at that same facility.

3 WHAT IS THE DIFFERENCE BETWEEN THE DOSSIER AND THE MEDICAL RECORD??

The dossier makes it possible to reconstruct the clinical history of a patient with reference to all the healthcare services provided to him/her by a given healthcare facility. The medical record, on the other hand, is a tool that describes, according to standards defined by the Ministry of Health, a single episode of hospitalisation of the person concerned.

4 WHO CAN THE HEALTH RECORD BE CONSULTED BY?

The dossier is accessible to all the health professionals of the health facility holding the dossier who will take care of the person concerned over time.

5 DOES THE PERSON CONCERNED HAVE THE RIGHT TO KNOW WHO HAS HAD ACCESS TO HIS OR HER HEALTH RECORD?

Yes. The Authority provided in the 2015 Dossier Guidelines that the data subject may request to know the accesses carried out on his or her dossier with an indication of the structure/department that carried out the access, as well as the date and time of the access.

6 DOES PROCESSING THROUGH A DOSSIER REQUIRE THE CONSENT OF THE DATA SUBJECT?

Yes. The informed consent of the person concerned must be obtained. However, it must be made clear (and the information notice must state this) that any failure to consent to treatment by means of the dossier does not affect the possibility of access to the medical treatment requested.

7 IS IT POSSIBLE TO WITHDRAW CONSENT TO THE HEALTH RECORD?

Yes. In the event of revocation, the dossier must not be further implemented, the information in it must remain available to the professional who compiled it, but it must no longer be shared with professionals in other departments who will subsequently take the person concerned into their care.

8 IN THE EVENT OF INCAPACITY OF THE PERSON CONCERNED, FROM WHOM MUST CONSENT TO THE FORMATION OF THE HEALTH RECORD BE ACQUIRED?

In this case, consent must be obtained from the person exercising legal authority over the person concerned. In the case of minors, upon reaching the age of majority, the consent of the person concerned must be obtained again.

9 ARE THERE ANY PROCESSING OPERATIONS FOR WHICH SPECIFIC CONSENT OF THE DATA SUBJECT IS REQUIRED?

Yes. The inclusion in the dossier of information subject to greater protection by the law (such as information relating to acts of sexual violence or paedophilia, HIV infection or the use of alcohol or drugs) must be expressly mentioned in the information notice and subject to the specific consent of the person concerned.

10 CAN THE PERSON CONCERNED REQUEST THAT CERTAIN INFORMATION ON HIS OR HER HEALTH NOT APPEAR IN THE HEALTH RECORD?

Yes. The person concerned may decide to obscure certain data or health documents, which will therefore not be visible and accessible via the file.

11CAN THE OBSCURATION REQUEST BE REVOKED?

Yes. Omission of the clinical event is revocable in time. If the person concerned has decided to withhold certain data or documents concerning him or her, this choice must not be inferred from the file.

12WHAT INFORMATION IN THE HEALTH RECORD CAN ADMINISTRATIVE STAFF ACCESS?

Administrative staff may only have access to administrative information that is strictly necessary to perform their functions (so-called 'modular access').