I.R.C.C.S. Ospedale San Raffaele	**Information for patients of Ospedale San Raffaele S.r.l. concerning the processing of personal data through Electronic Health Dossier pursuant to art. 13 and 14 Regulation (EU) 2016/679 (GDPR)**

Dear Madam / Dear Sir,

The Data Controller of personal data (the " **Data Controller** "), pursuant to art. 13 of Regulation (EU) 2016/679 (" **GDPR** ") and of the European and national legislation that supplements and / or modifies it, including Legislative Decree n. 196/2003 and subsequent amendments (hereinafter, " **Privacy Code** "), as well as the Guidelines on the subject of the Electronic Health Dossier of the Data Protection Authority of 4 June 2015 (" **DSE Guidelines** "), intends to provide you, in Your capacity of data subject (the " **Data Subject**"), the following information relating to the processing of personal data, to allow you to give a "free and informed" consent to the creation and consultation of an **Electronic Health Dossier** (" **DSE** ") which is going to collect, in digital format, your personal data (" **Personal Data** ") containing information on your state of health and/or sex life, relating to present and past clinical events, processed by the Data Controller, in order to document your health history . The logical sharing of this information in favor of all the health professionals who will take care of you would allow a complete and always updated view of your state of health, thus making the process of diagnosis and treatment more efficient. With your consent, the health dossier will also be available for consultation by professionals who operate in the intramural free profession or in the provision of services outside normal working hours using the Data Controller's outpatient and diagnostic facilities. For this reason, it is very important that, if you decide to give your explicit consent to the creation of your DSE, it is as complete as possible. In fact, you may request, at any time, the total blackout of some information, which you do not want to let any healthcare professional other than the one who treated you, or the partial blackout of some information, if you decide to let only some professionals view them and not others.

Contact details	
Data Controller	**Ospedale San Raffaele Srl,** with registered office in Milan, via Olgettina n. 60, 20132, tax code 07636600962, VAT number 07636600962 **E-mail address:** hsrsanraffaele@hsr.postecert.it
Data Protection Officer (RPD or DPO)	**E-mail address** : dpo@hsr.it

Personal data processed	
Data type	**Source**
Registry (name, surname, address, contacts, fiscal code etc)	Data collected from the data subject.
Health-related data ("Special categories of data")	
Data revealing racial or ethnic origin ("Special categories of data")	
Data revealing religious or philosophical beliefs ("Special categories of data")	
Data relating to sexual life/sexual orientation ("Special categories of data")	

Genetic data ("Special categories of data")	

Purpose of the processing	Legal basis of the processing	Data retention time
Creation and consultation of the patient's Electronic Health Dossier (DSE), in order to make the processes of prevention, diagnosis, treatment, rehabilitation and assistance or health or social therapy of the same within the health facilities of the Data Controller more efficient.	**Common data** Consent of the data subject, pursuant to art. 6, par. 1, letter a) of the GDPR. **Special categories of data** Consent of the data subject, pursuant to art. 9, par. 2 letter a) of the GDPR.	Until revocation of consent by the data subject.
Insertion in the DSE of clinical events prior to its establishment (e.g. reports, outpatient visits, hospitalizations, documentation provided or contained in the documents produced by the Structure before the date of issue of consent).	**Common data** Consent of the data subject, pursuant to art. 6, par. 1, letter a) of the GDPR. **Special categories of data** Consent of the data subject, pursuant to art. 9, par. 2, letter a) of the GDPR.	Until revocation of consent by the data subject.
Inclusion in the DSE of information subject to greater protection (information concerning acts of sexual violence, pedophilia, HIV infections, use of narcotic and psychotropic substances, alcohol, voluntary termination of pregnancy, parturient who request anonymity, services offered by family counseling).	**Common data** Consent of the data subject, pursuant to art. 6, par. 1, letter a) of the GDPR. **Special categories of data** Consent of the data subject, pursuant to art. 9, par. 2, letter a) of the GDPR	Until revocation of consent by the data subject.

Collection of consent

Consent for the processing of Personal Data through DSE by the health professionals who, from time to time, treat the data subject will be requested only at the first contact with the Hospital. For all subsequent health services, relating to the processing purposes referred to in this information notice, therefore, you will no longer be asked for your consent to the processing of Personal Data through DSE, which may take place until your consent is revoked.

The data subject will be able to choose, by issuing a specific and optional consent, whether or not he/she wishes to include the previous services within the established dossier and it is in any case his right to request the obscuring of certain data or health documents that can be consulted via DSE. In this case, the information and/or documents subject to blackout remain available to the healthcare professional or to the Data Controller's internal structure that collected or processed them (for example, a report accessible via DSE by the professional who drafted it; health record accessible from the relevant hospital department). The clinical documentation relating to the obscured event must in any case be kept by the Data Controller in compliance with the provisions of the sector legislation.

In any case, the consents you have given may be revoked pursuant to art. 7 of the GDPR at any time.

The consent given in relation to the processing of Personal Data of a minor by the legal guardian given expires with the coming of age for which it will have to be expressed again.

Without prejudice to the foregoing, we inform you that this information together with the consent you have given are effective with reference to the plurality of services also provided by each separate Operating Unit of the Data Controller.

Lastly, only if expressly and specifically permitted by the data subject, the DSE may also contain health information and/or documents relating to clinical services subject to greater protection listed in the table above.

Nature of the provision of data and consequences of any refusal

The granting of consent to the processing of data for the purposes indicated above is optional. Failure to consent does not prevent the data subject from accessing healthcare services, nor does it prevent the professional who is treating the patient from having access to the information provided at that moment by the patient and to that elaborated in relation to the clinical event for which the same requested a medical service. In the event of lack of consent, in fact, all the health services requested will still be provided to you and the Particular Data will, in any case, remain accessible to the health professional and/or to the ward/clinic/operating unit that prepared them, without their necessary inclusion in this instrument. However, it is considered appropriate to point out that, in this case, the healthcare professional or the ward/clinic/operating unit that will take care of you would not have all the information previously collected at the Data Controller's facility by other healthcare professionals and/or departments/outpatient clinics/operating units, potentially useful for assessing your state of health in a more complete way for the purposes of diagnosis and treatment.

Processing methods

The processing of Personal Data will take place - according to the principles of correctness, lawfulness and transparency - both in paper format and through IT and/or telematic supports and/or tools, with logic strictly related to the purposes of the processing and in any case guaranteeing the confidentiality and security of the data themselves and compliance with the specific obligations established by law.

The availability, management, access, conservation and usability of data is guaranteed by the adoption of technical and organizational measures to ensure suitable levels of security pursuant to articles 25 and 32 of the GDPR, as well as, in relation to the specific processing purposes identified by the applicable legislation, including the DSE Guidelines.

Consultation of the DSE will only be permitted during the period of time in which the healthcare service is rendered (and for a subsequent period of time not exceeding 45 days), after which it will no longer be possible to access the patient's DSE, unless this is deemed essential for the protection of the patient's health. In the latter cases, to monitor extraordinary accesses, the computer system will record the identification code of the person who logged in urgently (which must be expressly justified in writing) and the operations performed by the same (data entry, visualization, document printing, etc.).

To guarantee the confidentiality of the data and prevent their loss and theft, the system has in any case been equipped with suitable security measures which prevent unauthorized access - through authentication and authorization systems - and which automatically track the accesses made registering:

- the identification code of the person who connected to the system;
- the date and time of the connection;
- the code of the workstation used;
- the ID of the patient whose dossier is affected by the access operation;
- the type of operation performed on the data.

The operation logs will be kept for a period of no less than 24 months from the operation registration date.

Data communication

Your Personal Data will not be disseminated except in the case in which their communication or dissemination is required by virtue of legal provisions or orders from the authorities. In any case, these are subjects, bodies or authorities who act in their capacity as independent Data Controllers.

Data Processors
Your Personal Data may be communicated to service providers strictly related and functional to the activity of the Data Controller who typically act as data processors pursuant to art. 28 of the GDPR The complete list can be requested at any time from the Data Controller, by writing to the addresses indicated above.

Persons authorized to process
The processing is carried out by subjects duly authorized by the Data Controller and in compliance with the provisions of art. 29 of the GDPR. In particular, information regarding the state of health of the data subject is accessible to all health personnel specifically authorized pursuant to art. 29 of the GDPR and art. 2-quaterdecies of the Privacy Code which, for various reasons (e.g. specialist services, new hospitalization, rehabilitation activities, etc.) and over time, treat the patient, regardless of whether the service is provided under accreditation with the SSN or in a state of solvency (intramoenia freelance).

Transfer of personal data to countries outside the European Union
It is not the Owner's intention to transfer your Personal Data to Third Countries with respect to the European Union and the European Economic Area. Should this transfer become necessary and/or unavoidable due to organizational needs of the Data Controller, it is hereby announced that it will take place exclusively to countries for which there is an adequacy decision adopted by the European Commission; if it is a country other than the one referred to in the previous point, the transfer of data will be governed by the Standard Contractual Clauses without prejudice to the adoption, with the prior agreement of the Parties involved, of another of the safeguard measures established by art. 46 of the GDPR or from the application of one of the derogating mechanisms pursuant to article 49 of the GDPR.
More information is available from the Data Controller by writing to the addresses indicated above.

Rights of the data subject
In relation to the processing of your personal data, you will be able to assert the rights granted to the data subject by art . 7 (right to withdraw consent), and by articles from 15 to 22 of the GDPR, where applicable and within the limits established by art. 2-undecies of the Privacy Code (right of access to data, right of rectification or cancellation of the same, right of limitation to the processing or opposition to the same, right to data portability, right not to be subjected to an automated decision-making process) , by forwarding a written request to the Data Controller or to the DPO at the addresses indicated above.
We also inform you that pursuant to art. 140-bis of the Privacy Code, you can lodge a complaint with the Data Protection Authority (Garante Privacy) or appeal before the judicial authority.

Furthermore, the data subject has the right to:

- request, at any time, that the consultation of certain information and/or health documents, relating to clinical events concerning him, be limited to some doctors, specifically authorized by the data subject;
- view the accesses to the health dossier. In particular, the data subject may ask the Data Controller to find out what accesses to his DSE have been, with an indication of the Operating Unit and/or the professional who carried them out, as well as the date and time of the same;
- request, at any time, **the obscuring of certain information and/or health documents relating to clinical events concerning him** (for example an emergency room service, hospitalization, a specialist service, etc.), or that the same are not included in the DSE or that they are viewed only by certain professionals. The blackout request, which may be revoked over time, will not be brought to the attention of anyone authorized to access the DSE (so-called " **blackout** "). In any case, we inform you that the obscured events will always be accessible by the Operating Unit (in the case of hospitalization) or by the professional (in the case of an outpatient visit, even in a state of solvency) who generated the obscured document;

- revoke the consent at any time, without prejudice to the lawfulness of the processing based on the consent given before the revocation. In case of withdrawal of consent, the DSE will not be implemented further and its display will no longer be allowed until possible new consent. However, the health information remains available to the professional or to the ward/outpatient clinic/operating unit that prepared it (e.g. information relating to a hospitalization that can only be used by the inpatient ward) and/or to fulfill any retention obligations established by law , but must no longer be shared with the professionals and/or other departments/outpatient clinics/Operational Units who will subsequently take care of the data subject.

Requests must be addressed in writing to the Data Controller or to the DPO at the addresses indicated above.

Date of last update: July 2023