Information for patients of Ospedale San Raffaele S.r.l.
concerning the processing of personal data pursuant to art. 13 and 14 Regulation (EU) 2016/679 (GDPR)

Dear Madam / Dear Sir,

The Data Controller of personal data (the " **Data Controller** ") intends to provide you, in your capacity as data subject (the " **Data Subject** "), with the specific information on the processing of your personal data (" **Personal Data** ") which is necessary with reference to the activities carried out within the Data Controller's healthcare facility in its various hospital or territorial divisions, pursuant to articles 13 and 14 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** ").

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 (DPO) E-mail address : dpo@hsr.it

Personal data processed	
Data type	**Source**
registry	Data collected from the data subject or, through the exercise of the services provided by the structure, from third parties, such as, for example: family members of the patient; subjects who legally exercise parental authority, guardianship or legal representation with respect to the patient; healthcare facilities or third-party specialists.
Email, internet browsing, operations on IT systems	
Data revealing racial or ethnic origin	
Data revealing religious or philosophical beliefs	
Genetic data	
Health data	
Data relating to sexual life/sexual orientation	

Purpose of the processing	**Legal basis of the processing**	**Data retention period**
Purpose	**Legal basis**	**Storage time**
A. Prevention, diagnosis, treatment and rehabilitation activities, including diagnostic, therapeutic, laboratory services, specialist outpatient services, hospitalization, continuity of care after discharge	**Common data** Execution of a task of public interest or connected to the exercise of public powers vested in the Data Controller, *pursuant to* art. 6, par. 1, lit . e) of the GDPR **Particular categories of data** Purposes of diagnosis, assistance or health or social therapy or management of health or social systems and services on the basis of Union or Member State law or in accordance with a contract with a health professional, *pursuant to* art. 9, par. 2, lit . h) of the GDPR	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.

B. Administrative and certification activities strictly connected to the achievement of the purposes of prevention, treatment, diagnosis, rehabilitation and assistance or health or social therapy (for example to manage reservations, patient acceptance, compilation of medical records and other documentation, for the management of payments, to receive sms of remainder reservations, to allow the provision and functioning of the queue elimination service provided at the Company's offices)	**Common data** Execution of a task of public interest or connected to the exercise of public powers vested in the Data Controller, *pursuant to* art. 6, par. 1, lit . e) of the GDPR **Particular categories of data** Reasons of significant public interest on the basis of Union or Member State law, *pursuant to* art. 9, par. 2, lit . g), of the GDPR in conjunction with the art. 2-sexies, of the Privacy Code	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
C. Fulfillment of obligations established by laws and regulations, as well as execution of provisions issued by the Authorities or by supervisory, control and reporting bodies (for example, the sending of information to the competent bodies of the NHS and SSR, social security and welfare bodies, Insurance companies, in limits to the performance of their institutional task)	**Common data** Fulfillment of the legal obligations to which the Data Controller is subject *pursuant to* art. 6, par. 1, lit . c) of the GDPR **Particular categories of data** Reasons of significant public interest on the basis of Union or Member State law, pursuant to art. 9, par. 2, lit . g) of the GDPR in conjunction with art. 2-sexies, of the Privacy Code	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
D. Carrying out tasks of the national health service and of subjects operating in the health sector, as well as tasks of hygiene and safety in the workplace and safety and health of the population, civil protection, protection of life and physical safety	**Common data** Execution of a task of public interest or connected to the exercise of public powers vested in the Data Controller, *pursuant to* art. 6, par. 1, lit . e) of the GDPR **Particular categories of data** Reasons of public interest in the public health sector, such as protection from serious cross-border threats to health or the guarantee of high standards of quality and safety of health care and medicines and medical devices, pursuant to *art* . 9, par. 2, lit . i) of the GDPR	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
E. Management of pharmacovigilance and reporting of adverse events (reactions to therapies, drugs, reports of infectious diseases, etc.)	**Common data** Execution of a task of public interest or connected to the exercise of public powers vested in the Data Controller, pursuant *to* art. 6, par. 1, lit . e) of the GDPR **Particular categories of data** Reasons of public interest in the public health sector, such as protection from serious cross-border threats to health or the guarantee of high standards of quality and safety of health care and medicines and medical devices, *pursuant to* art. 9, par. 2, lit . i) of the GDPR	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
F. Management of complaints and reports from users	**Common data**	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*",

	Execution of a contract in which the data subject is a party or of pre -contractual measures, *pursuant to* art. 6, par. 1 letter . b) of the GDPR **Particular categories of data** Purposes of diagnosis, assistance or health or social therapy or management of health or social systems and services on the basis of Union or Member State law or in accordance with a contract with a health professional, pursuant to *art* . 9, par. 2, lit . h) of the GDPR	approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
G. Possible communication of clinical documentation of the patient/insured to insurance companies limited to the object of the insurance relationship existing between the data subject and the insurance company	**Common data** Execution of a contract of which the data subject is a party pursuant to art. 6, par. 1, lit . b) of the GDPR **Particular categories of data** Consent of the data subject, *pursuant to* art. 9, par. 2, lit . a) of the GDPR	Times established in the "Version 04" of "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia*", approved with Decree of the DG Welfare n. 15229 of 1 December 2017 and subsequent amendments, adopted by the Lombardy Region which applies to the entire Lombard social and health system.
H. Carry out satisfaction surveys on the health services used (so-called "customer satisfaction ") and in order to improve the quality of the services themselves. The Personal Data collected through the questionnaires are destroyed or made anonymous immediately after their collection.	**Common data** Consent of the data subject, *pursuant to* art. 6, par. 1 letter . a) of the GDPR **Particular categories of data** Consent of the data subject pursuant to art. 9, par. 2 lit. _ a) of the GDPR	Times strictly necessary to anonymize or destroy the data present in the questionnaires and in any case no later than 3 months.
I. Communication of information on the patient's state of health or on his presence in the structure to third parties (e.g. family members or acquaintances), specifically indicated by the same.	**Common data** Consent of the data subject, *pursuant to* art. 6, par. 1 letter . a) of the GDPR **Particular categories of data** Consent of the data subject, *pursuant to* art. 9, par. 2, lit . a) of the GDPR	Up to the moment of the possible revocation of the consent by the data subject
J. Sending promotional communications and direct marketing, including the sending of newsletters, through automated tools (such as SMS, email, push notifications, MMS, telephone without operator) and not (ordinary mail, telephone with operator).	**Common data** Consent of the data subject, *pursuant to* art. 6, par. 1 lit. a) of the GDPR	Up to the moment of the possible revocation of the consent by the data subject.
K. Communication of Data to GSD Sistemi e Servizi Sc a rl ("GSDSS") to allow the latter to pursue the purpose of group marketing, promotion and information in the clinical/scientific field as independent data controller, as well as to raise awareness raising funds for the support and development of scientific research.	**Common data** Consent of the data subject, *pursuant to* art. 6, par. 1 lit. a) of the GDPR	Once acquired and subject to your consent, the Personal Data will be immediately communicated to GSDSS, which will process them for the purpose described until the moment of the possible revocation of consent by the data subject

L. Communication of Personal Data , including those relating to your health, to GSD Sistemi e Servizi Sc a rl ("GSDSS") , to allow the latter to send you , as independent data controller, promotional communications of the services offered by the group, personalized and also focused on prevention and follow-up paths in the best interest of the patient and which will be sent by ordinary mail, text message and email.	**Common data** Consent of the data subject, *pursuant to* art. 6, par. 1 lit. a) of the GDPR **Particular categories of data** Consent of the data subject, *pursuant to* art. 9, par. 2, lit. a) of the GDPR	Once acquired and subject to your consent, the Personal Data will be immediately communicated to GSDSS, which will process them for the purpose described until the moment of the possible revocation of consent by the data subject
M. Purpose of retrospective scientific research related to the pathology for which the patient is being treated at the hospital. As an IRCCS the Hospital is authorized by law to be able to further process the data originally collected for healthcare activities for the further purpose of scientific research. In any case, the data processing, depending on the research project carried out, may take place with pseudonymous data (indirectly attributable to Your person). Further detailed information will be made available on the hospital website in the appropriate section.	**Common data** Execution of a public interest task of the IRCCS in the context of scientific research as a collective contribution pursuant *to* art. 6, par. 1 lit. e) of the GDPR **Particular categories of data** Scientific research purposes *pursuant to* articles 9, par.2, lett. g) and 89 of the GDPR as well as on the basis of the provisions of national law regarding the IRCCS pursuant *to* art. 110 bis, par. 4, of the Privacy Code	At any time, the Personal Data collected for clinical purposes may be used for research projects. The retention times for these purposes will be explained in the information relating to the individual research protocols
N. Personal Data may be made effectively and irreversibly anonymous in order to allow their use in future research projects		Your Personal Data will be kept only for the time necessary to carry out the anonymization process.
O. Ascertainment, exercise or defense of the rights of the Data Controller, including the exercise of a debt collection action against the data subject	**Common data** Pursuit of the legitimate interest of the data controller, *pursuant to* art. 6, par. 1, lit. f) of the GDPR **Particular categories of data** Assessment, exercise and defense of a right in court *pursuant to* art. 9, par. 2, lit. f) of the GDPR	For the entire duration of the dispute, until the time limits for appeal actions have expired.
P. Recontact of the patient by e-mail, in relation to health treatments already received, also with prevention purposes to be implemented on a periodic basis, as well as for promotion and information activities of services similar to those already received.	**Common data** Pursuit of the legitimate interest of the data controller, pursuant to art. 6, par. 1, letter f) of the GDPR in conjunction with art. 130 paragraph 4 of the Privacy Code.	Until the moment You declare that you no longer want to receive the e-mails described from the Data Controller. To this end, you can contact the Data Controller or the DPO, writing to the contacts listed in the epigraph or you can click the link for unsubscribing that you will find under each e-mail.

Personal Data collected for the purposes of prevention, treatment, diagnosis, rehabilitation and medical or social assistance or therapy will be processed by or under the responsibility of a professional subject to professional secrecy or by other persons subject to the obligation of secrecy in accordance with the law of the European Union or national law or the rules established by the competent national bodies, *pursuant to* art . 9, par. 3, of the GDPR. With regard to the retrospective scientific research activity, the Data Controller is a Scientific Hospitalization and Care Institute (IRCCS) which carries out a prevalent scientific research activity which it intends to pursue also through the further processing of Personal Data collected for clinical activity . You can request and access any further information by contacting the Data Controller and the DPO directly at the respective e-mail addresses. Each scientific research project is accompanied by specific

documentation that you can access upon request and available in a specific section of the hospital website, in accordance with the provisions of national and European legislation, including sectoral ones.

Electronic Health Record
We inform you that with your explicit consent you can make your Personal Data and health documents available, which are formed, integrated and updated over time by several subjects, in order to document, in perspective, your entire clinical history, through the tool of the Electronic Health Record. For further information on the Electronic Health Record, consult the information on the processing of personal data for the Electronic Health Record of the Lombardy Region available on the website: https://www.fascicolosanitario.regione.lombardia.it/privacy
To give, revoke consent and manage the authorizations relating to your Electronic Health Record, you can access online through the Electronic Health Record website of the Lombardy Region (https://www.fascicolosanitario.regione.lombardia.it/fascicolo) or via the Electronic Health Record APP https://www.fascicolosanitario.regione.lombardia.it/app .

Nature of the provision of data and consequences of any refusal
The provision of Personal Data required for health care and administrative purposes strictly related to these is essential; failure to provide it could make it impossible for the data subject to access health services.
Failure to consent to the processing of Personal Data for the other purposes indicated above does not prevent access to the health service, but will make it exclusively impossible for the Data Controller to carry out the related processing.

Processing methods
The processing of Personal Data will take place - according to the principles of correctness, lawfulness and transparency - both in paper form and through IT, manual and/or telematic supports and/or tools, with logic strictly related to the purposes of the processing and, in any case, guaranteeing confidentiality and security of the data itself 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.

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. Furthermore, where you have given specific consent, your Personal Data will be communicated to GSDSS which will process them as independent Data Controller for marketing purposes.

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 Personal Data may be processed by employees of the corporate functions responsible for pursuing the aforementioned purposes, who have been expressly authorized for processing and who have received adequate operating instructions in compliance with the provisions of art. 29 of the GDPR.

Transfer of personal data to countries outside the European Union
It is not the Data Controller'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.