

INFORMATION ON THE PROCESSING OF PERSONAL DATA PATIENTS

Information on the processing of personal data in the health sector for the clients of Dr Stefania Paesani (PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 27 APRIL 2016 - RGPD)

Dear Madam(s),

Dr. Stefania Paesani (hereinafter, for brevity, also "Dr. Paesani"), in accordance with the provisions of Regulation (EU) 2016/679 (hereinafter briefly referred to as "GDPR"), as the Data Controller of Personal Data (hereinafter, for brevity, the "Data Controller"), provides you with the following information regarding the processing of your Personal Data in accordance with the rules set forth in the GDPR and the European Union and national legislation supplementing and/or amending it ("Applicable Privacy Legislation").

The information provided by the Data Controller herewith refers to the data provided by you, or otherwise acquired by Dr. Paesani, with reference to the activity that may be exercised within the offices in which he receives, as it is related to the prevention, diagnosis, treatment, assistance, health therapy and rehabilitation services that you may require.

According to the provisions indicated, the processing will be based on the principles of correctness, lawfulness, transparency in compliance with the guarantees of confidentiality and protection of your rights.

Personal Data Controller

Stefania Paesani, with registered office in Via Como, 38, 22070, Rovello Porro (CO), in the person of its pro-tempore legal representative. The owner can be contacted by PEC at stefania.paesani.oebv@co.omceo.it . Those who do not have a PEC (certified electronic mail) address but a normal mailbox can write to the address: info@stefaniapaesani.it

Data Protection Officer ('DPO')

The Controller has not designated a Data Protection Officer ('DPO').

Types of data processed

The data subject to processing, which you provide to the Controller, or which are otherwise acquired by the Controller, in order to use the services are/will be:

- 1 Common Personal data (e.g. first name and surname, date of birth, address of residence and/or domicile, other data of a personal nature);
- 2³ Personal data relating to particular categories (e.g. and in particular health-related data): Data relating to your state of health provided by you directly, or possibly collected from third parties, in accordance with the law, or acquired by the data controller (including through health documentation) in the course of inspections or visits.

Data allowing the disclosure of racial or ethnic origin, religious or philosophical beliefs, data concerning a person's sexual life or sexual orientation may be processed for the achievement of the purposes of the specific processing, within the framework of the institutional purposes attributed to the Data Controller, or in the cases provided for by laws or regulations.

The aforementioned personal data will hereinafter be jointly referred to as 'Personal Data', unless otherwise specified.

They could also be treated:

- Personal Data for access to telematic services on behalf of the Controller: Personal Data will be processed for registration and the use of related services, including the possibility of requesting reports, or other online health documentation.
- ⁴Genetic data : data will possibly be processed limited to information and operations that are indispensable to protect the physical safety and health of the data subject, a third party or the community. The processing of genetic data will only be permitted in the cases and ways provided for by the GDPR and the legislation

¹ 'Personal data' means any information relating to a natural person who is identified or identifiable, even indirectly, by reference to any other information, including a personal identification number.

² Pursuant to Article 9(1) of the GDPR, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sex life or sexual orientation are to be understood as

³ 'Health-related data' means personal data relating to the physical or mental health of a natural person, including the provision of health care services that reveal

or health of that natural person and that result in particular from the analysis of a biological sample of that natural person.

privacy applicable and in accordance with the guarantee measures ordered by the Italian DPA, in compliance with laws and regulations.

- Personal data and health-related data concerning family members of the person assisted, only if strictly necessary in the opinion of the health professional responsible for the person's care.
- Personal data concerning the family members of the person assisted, or the guardian, the exerciser of parental authority (of the minor), the support administrator, the legal representative of the person concerned, when required for the provision of services or for the purpose of access to data concerning the health of the person concerned, or necessary for the communication of the state of health of the person concerned.

Purpose and legal basis of processing

The Data Controller will process your Personal Data for the performance of the firm's institutional functions, within the scope of the performance of public interest tasks, in compliance with the applicable privacy legislation and the specific provisions of the sector.

The Controller processes your Personal Data lawfully, pursuant to Article 6 of the GDPR, where the processing:

- is necessary for the achievement of the institutional purposes attributed to this Controller by the national and regional legislation in force and for the performance of the services concerning you or optionally activated by you, by virtue of which the processing is carried out;
- is necessary for reasons of substantial public interest within the meaning of Art. 9(2)(g) of the GDPR, on the basis of European Union law, or national law (if provided for by law, or in cases provided for by regulation), for the performance of related tasks in particular in the health sector and for related administrative purposes, in accordance with Art. 2 - sexies of the 'Personal Data Protection Code';
- is necessary to comply with a legal obligation to which The Controller is subject;
- is based on express consent to the processing of the data, where required by the controller (in the cases described below), freely given.

In particular, your Personal Data, as part of the provision of services during your visits with Dr. Paesani, are/will be processed for the following purposes

- a) prevention, diagnosis, treatment, health or social care or therapy and rehabilitation and administrative-accounting activities connected with or instrumental to the management of relations with the assisted person (e.g. booking of visits and examinations, outpatient services, for the collection/delivery of reports) and certification activities relating to health status, including those related to specialist therapies and child neuropsychiatry treatments;
- b) purposes connected with the tasks of the National Health Service, as well as tasks relating to hygiene and safety in the workplace and the safety and health of the population, civil protection, epidemiological surveillance, monitoring of risk groups, safeguarding the life and physical safety of the person concerned or of third parties or the community;
- c) if a foreigner, health and related administrative purposes relating to the provision and registration of assistance to foreigners in Italy;
- d) health care planning, monitoring, management and evaluation, also carried out by means of satisfaction surveys and questionnaires;
- e) photographic and video footage for therapeutic purposes;
- f) photographic and video shooting for recreational purposes;
- g) defensive, administrative and judicial protection purposes concerning the holder;
- h) activities in compliance with obligations under laws, regulations and EU legislation (e.g. administrative checks).

It is also possible that your Personal Data are/will be processed for other purposes:

- i) to provide other goods or services to the data subject via an electronic communications network;
- j) for promotion or information activities in the clinical/health/scientific field, excluding any particular personal data, only with your consent;
- k) didactic activities, education, training and professional information in the field of health of the authorised holder's personnel, studies of pathologies (in all these cases in compliance with your rights);
- l) for scientific purposes, including scientific research and controlled clinical trials of medicinal products, in accordance with laws and regulations, subject, where required, to your consent,
- m) in the context of tele-assistance or telemedicine, for health care, subject, where required, to your consent;
- n) for scientific research activities in the medical, biomedical and child neuropsychiatric fields, subject, where necessary, to your consent for the processing of data disclosing your state of health (see Article 110 of the Privacy Code); or for statistical purposes. The processing of personal data for scientific research or statistical purposes will be carried out in compliance with the guarantees

of the data subject's rights (e.g. the principle of data minimisation), within the limits and in the manner provided for in Article 89 of the GDPR, in accordance with laws and regulations (in this case in anonymous or aggregate form).

Treatment modalities

In relation to the purposes described above, the Data Controller will process your Data by means of manual, computerised and telematic tools, with logic strictly related to the purposes of the processing, so as to guarantee the confidentiality and security of the same, in compliance with the rules laid down under the GDPR and current legislation.

Data may also be collected by means of photographic images, video recordings or other computer media during behavioural therapies, outpatient visits or at the discretion of the health management.

In addition to specific health care and protection purposes, they may be used for scientific research purposes, unless you wish otherwise, or for the purposes of professional training of doctors, health care workers in general or students, collaborators and professionals attending courses of study or lectures, subject to your specific consent in those exceptional cases where the processing of data in anonymous form cannot be guaranteed.

The data will be processed exclusively by persons (staff and collaborators of The Controller) specifically authorised to do so, in compliance with Article 29 of the GDPR. On behalf of the Controller, the data may be processed by the subjects designated as data processors within the scope of the contract that punctually regulates the processing entrusted to them, pursuant to Art. 28 of the GDPR. The data controller or data processor may provide, that specific tasks and functions related to the processing of personal data are attributed to natural persons, expressly designated, operating under their authority, pursuant to art. 2-quaterdecies of Legislative Decree 10 August 2018, no. 101 (Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679).

The facebook page, mobile phone (e.g. whatsapp), email and similar tools are not considered suitable for processing personal data, especially when they relate to the health of a data subject and are therefore of a special nature. The owner advises not to use these channels to communicate with Dr Paesani except solely to make an appointment.

Nature of processing and acquisition of consent to provide Data

The provision of your Personal Data, requested from time to time, is necessary for the achievement of the institutional purposes attributed to the Data Controller by current national and regional legislation (in particular, for example, by Law 833/78, Legislative Decree 502/92 and subsequent amendments and additions, LL.RR. 8/95 and by the D.P.C.M. 29/11/2001), as well as for the achievement of the processing purposes.

In this sense, failure to provide Personal Data, except in cases of urgency and/or medical emergency, makes it impossible for the person concerned to access the health service.

With regard to the freely given consent, the acquisition of consent is not necessary, pursuant to Order No. 55 of 7 March 2019, for the following cases:

- the processing of your common and special personal data, including those relating to your state of health for the achievement of the health purposes of prevention, diagnosis, treatment and rehabilitation and related administrative activities and for the other purposes set out above in the context of the institutional functions attributed to the Data Controller and related activities, with the exception of all cases that, according to current legislation, fall within the concept of 'state of necessity';

With regard to the freely given consent, the acquisition of consent is necessary (pursuant to Art. 9, Section 2 a) of the GDPR) for the following cases:

- for the communication of information on your state of health to third parties (e.g. family members or acquaintances) specifically indicated by you;
- the possible transfer of personal data to a third country, including a non-EU country, or an international organisation, in the absence of legal requirements concerning the adequate level of data protection and in implementation of the data subject's protection guarantees set out in the GDPR;

Consent is, however, optional, where required, for:

- o Promotional activity, sending (e.g. by sms, e-mail or regular mail) communications, information/promotional material, concerning, for instance, news on research, therapeutic innovation or for the communication of events or other information initiatives.

Consent is not required for Personal Data processed by the Data Controller for the fulfilment of institutional purposes, in compliance with the obligations provided for by laws, regulations and EU legislation (e.g. for purposes related to the tasks attributed to the NHS, or for inspection tasks attributed as a body in charge of health supervision)

Upon acceptance, the Controller's staff and/or other collaborators authorised to process data by the Controller, will ask you/they will ask you to give specific consent to the processing of your data, as applicable.

Only the data subject to whom the health data relate shall give consent or revoke it. If the person concerned is a minor or a person under guardianship, only the person exercising legal representation may give consent or revoke it.

Consent is given upon first access to one of our facilities and is valid until revoked. In order to avoid repeated requests for 'Consent to the Processing of Personal Data', you will therefore no longer be asked for consent to process the relevant data for all services after your first access.

Notwithstanding the foregoing, we inform you that this information notice together with the consent given by you shall be effective with regard to the plurality of services (outpatient services, diagnostic examinations, admissions, boarding and semi-boarding stays) provided even at different times and even by different departments or outpatient clinics of the Holder.

The compulsory or optional nature of the provision of data will in any case be specified at the time of collection.

Categories of recipients to whom the data may be disclosed

For the achievement of the purposes set out above, in order to comply with specific legal obligations, the personal data processed, or some of them, may be transmitted to parties to whom communication is required by national or European Union law or regulation, or on the basis of existing legal relationships with The Controller. In particular, the data may be communicated to:

- o natural persons authorised by the Data Controller to process personal data pursuant to Article 29 of the GDPR by reason of the performance of their work duties within the Data Controller's facilities (e.g. medical and paramedical staff who, also at a later stage, will provide healthcare services in favour of the data subject, and administrative staff), who may pass them on to other authorised parties in compliance with professional secrecy;
- o to other public and private health authorities (e.g. nursing homes) and to the region to which the user belongs;
- o the central and peripheral bodies of the State;
- o to social security and welfare institutions as appropriate;
- o to other public entities (e.g. region, municipality) or private entities (entrusted with tasks by the ASL), for institutional and welfare purposes (e.g. hygiene, public health, health care and expenditure control, transport);
- o third parties, including private parties, in a contractual or contractual relationship with the Controller who are entrusted with tasks by the ASL (e.g. consultants, freelance professionals)
- o the Judicial Authority and/or the Public Security Authority, in the cases expressly provided for by law;
- o service providers (e.g. the company that manages the medical records archive, the company that manages telephone confirmations of bookings for examinations and/or visits) who typically act as data processors pursuant to Article 28 of the GDPR) for activities strictly related and functional to the Controller's business.
- o to appointed parties (insurance and non-insurance) for the protection of the organisation itself and its operators in the event of liability or for the purpose of ascertaining the right to compensation for damages of the injured user;
- o associations and foundations, voluntary organisations, social workers, as appropriate.
- o Consultants and/or freelancers in individual or associated form, Central Accountability System (TS System), Medical Records Software Companies also in Cloud

The scope of the communication may be extended to entitled third parties and to anyone the person concerned expressly indicates such as family members, attending physician. In the event of hospitalisation, the person concerned has the right to request that no information about his or her presence in hospital and the location of the hospitalisation be released.

Apart from these cases, the data will not be communicated to third parties or disseminated, except in cases specifically provided for by national or European Union law.

Reservations

In relation to the "Book on line" service, the external website www.miodottore.it is to be considered an autonomous, independent data controller, to which Dr Paesani does not confer any data. Any patient, interested in the processing of personal data, who freely chooses to turn to this provider for the booking service is invited to consult the information notice of the data controller. The Vercelli Medical Practice and the AIMC are to be considered autonomous data controllers in the same way.

Transfer of personal data to a recipient in a third country.

Your Personal Data will be processed within the European Union. If required by a specific legal provision or if it is necessary to fulfil a contractual obligation to a data controller or for the purposes of health protection, or research and experimentation, your Personal Data or some of your Personal Data may be transmitted to third countries outside the European Union or to an international organisation, provided that an adequate level of protection is guaranteed, in accordance with the rules set out in Chapter V of GDPR EU 2016/679 (Art. 44 et seq.).

In particular, we would like to inform you that the transfer of your data outside the European Union, in the absence of an adequacy decision by the European Commission, or other appropriate measures as provided for by the GDPR, will only be carried out if you have explicitly consented to it. Further information is available from the Data Controller by writing to the above addresses.

Data retention.

Your personal data, subject to processing for the purposes indicated above, will be stored in compliance with the principles of necessity and proportionality, within the timeframe and in the manner established by national reference legislation and, in any case, for as long as the Data Controller is subject to data storage obligations for purposes related to the institutional functions of the Data Controller, in accordance with the law or regulations.

Rights of the data subject.

The full list of Data Processors for the Controller is available from the Controller. Pursuant to the Regulation (Articles 15 et seq. of the GDPR), the data subject has the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning him or her, or to object to the processing of personal data, as well as the right to data portability. The data subject is granted all the rights referred to in Chapter III "Rights of the data subject" of the Regulation and the right to lodge a complaint with a supervisory authority (the independent public authority established by a Member State - in Italy the Italian Data Protection Authority) in accordance with the procedures laid down.

Other information

DELIVERY OF REPORTS

The reports of medical/health services rendered may only be delivered to the person concerned or to persons authorised or delegated in advance by filling in the appropriate forms provided by The Holder.

COMMUNICATION TO FAMILY MEMBERS OR THIRD PARTIES OF ITS PRESENCE AT THE HOLDER'S PREMISES

In the event of hospitalisation, the staff or collaborators of Data Controller will inform the persons requesting it of your presence, unless you indicate otherwise on the appropriate forms.

This privacy policy was last updated in February 2019.