DOMANDE PROVA ORALE DIRIGENTE ANALISTA (COD. 18/2025)

PROVA ORALE N. 1

- Descrivere in termini generali che cosa si intende per software di "middleware", ed esporre le sue caratteristiche peculiari.
- Com'è il suo approccio dovendo comunicare dati molto tecnici a interlocutori non tecnici, ad esempio clinici?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 2

- Esporre le differenze che caratterizzano la firma elettronica, la firma elettronica avanzata e la firma elettronica qualificata.
- Come approccia la gestione di una conflittualità importante con un suo collaboratore
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 3

- Descrivere che cosa si intende per Dossier Sanitario Ospedaliero e le principali differenze con Il Fascicolo Sanitario Elettronico.
- Come pensa sia il modo migliore per affrontare delle resistenze interne all'introduzione di un nuovo progetto?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 4

- Descrivere la MFA e le sue funzioni.
- Supponga di dover gestire un servizio con una alta conflittualità interna, qual è il suo approccio e la prima cosa che farebbe?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 5

- Business continuity e disaster recovery: descrivere i possibili approcci.
- A fronte di una innovazione tecnico – gestionale molto complessa da avviare, qual è il suo modo di approcciarsi?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 6

- Descriva brevemente i tre modelli di cloud IaaS, PaaS e SaaS, indicando le opportunità e limiti per ciascun modello.
- Come pensa di motivare un team in un contesto di risorse economiche limitate?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 7

- Indicare quali sono i requisiti normativi essenziali per l'affidamento di un servizio Cloud per la PA ed in particolare per i dati sanitari.
- Come si approccia nella collaborazione ad un nuovo progetto con altre strutture tecnico/ amministrative della stessa organizzazione

- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 8

- Descrivere i principali standard di interoperabilità in uso nel contesto sanitario e gli ambiti di applicazione.
- Come pensa di gestire un team con performances lavorative molto diverse tra di loro?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi / insuccessi raggiunti dall'organizzazione di appartenenza.

PROVA ORALE N. 9

- Indicare quanti sono i livelli EMRAM e quali sono i principali elementi che li contraddistinguono.
- Come pensa di gestire le risorse del suo team in un contesto di risorse scarse e di una pluralità di progetti da ultimare?
- Descriva una sua esperienza lavorativa che ritiene degna di essere narrata per risultati ottenuti in termini crescita professionale, oppure di successi/insuccessi raggiunti dall'organizzazione di appartenenza.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Guidelines on the Electronic Health Record and the Health File

[doc. web n. 1608673]

Guidelines on the Electronic Health Record and the Health File
(As published in Italy´s Official Journal no. 71 dated 26 March 2009)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Table of Contents

1. E-Health: An Overview

Several initiatives have been undertaken to deliver more effective health care by developing electronic networks further and expanding the computerised management of records, documents and processes in connection with upgrading private and public health care.

This is the context applying to a few initiatives that are aimed at storing, with the help of different techniques, the multifarious documents used by health care bodies for different treatment-related purposes; reference can be made, for instance, to the recent experience related to computerisation of medical records, which are actually regulated by specific legislation. Processing of the personal data that may be used in that respect is already regulated by the Data Protection Code (see, in particular, sections 75 et seq. and section 20 thereof).

Alongside these initiatives of a general nature there are some that have been coming up of late in respect of more specific topics; they also have to do with the modernization of health care, however they feature some peculiarities that point to the advisability of addressing them on a separate count.

The innovation to be addressed specifically here has to do with the sharing of health care data and

records by several organizations and/or professionals via computerised means; such data and records may be created, supplemented and updated over time by various entities in order to document a whole gamut of health events concerning the given individual as thoroughly as possible in accordance with a unified approach – ultimately, that individual's medical history as a whole can be documented.

The data and records in question may feature different characteristics and/or put emphasis on different aspects; they have long been the focus of attention in connection with the so-called electronic health record (hereinafter, EHR) and the so-called health file (hereinafter, HF). In the Guidelines developed below, reference is made as for both the EHR and the HF to the various clinical events concerning a given individual insofar as those events are shared logically by the professionals and/or health care organizations treating and/or supporting that individual in order to provide better care.

The peculiar features inherent in the circumstance that several entities share sensitive medical information documenting medically relevant events that have affected an individual over a given time span calls for specific considerations as opposed to those concerning the paper-based management of similar records and, more generally, the computerisation of health care.

Pending the enactment of legislation regulating a few basic issues, the Italian DPA considers it appropriate to lay down an initial set of precautionary measures to timely highlight specific safeguards and responsibilities and outline the applicable rights.

2. Scope of the Guidelines

There is no primary or secondary legislation regulating the EHR and/or the HF at national level; accordingly, it is necessary to rely on a commonly agreed definition by drawing inspiration, inter alia, from the work done in this respect by the Article 29 Working Party.

The considerations made herein apply to the EHR and the HF insofar as they represent a set of medical data relating, as a rule, to a given individual and contained in several inter-linked electronic records that can be shared by various public and private health care bodies.

Both the EHR and the HF contain several items of information on an individual's health that relate to current and past clinical events (e.g.: medical findings; hospitalization records; emergency care) and are aimed at documenting that individual's medical history. The personal data are inter-linked via different computerised tools, which in any case allow the data to be easily retrieved and browsed by the various health care professionals and/or bodies providing medical care to that individual over time.

Based on the findings gathered at national level, in particular the considerations made by the working group set up at the Ministry of Labour, Health and Welfare with a view to introducing a national Electronic Health Records system, the set of medical data at issue is referred to differently in these Guidelines depending on the respective scope of operation. More specifically, the Health File is a file set up at a health care body that acts as the sole data controller (e.g., a hospital or a nursing home) where several health care professionals are employed. Conversely, the Electronic Health Record is a file set up by pooling the data from different data controllers, which as a rule – though this is not always the case – operate within the same geographical area (e.g., a health care unit and a private laboratory operating in the same Region and/or area). For instance, health files may also make up the set of health care information held by the individual data controllers that participate in an EHR initiative at regional level.

The Electronic Health Record should be set up by prioritizing solutions that do not entail

duplication of the medical information created by the health care professionals/bodies that have treated the given data subject.

Secondly, since the medical data and documents contained in a EHR are collected from different sources, the appropriate measures should be taken to allow tracing back the entities responsible for creating and collecting the data and making them available via the EHR – also with a view to accountability.

Regarding the EHR, since separate clinical records are at issue, it should be ensured that each entity that has created/drafted those records continues to be, as a rule, the sole data controller in their respect – even though the information is made available to the other entities that are authorised to access the EHR. Availability is often achieved, for instance, by allowing all the entities that have treated the given data subject to share the list of the relevant clinical events; such list is at times set up in the form of an index and/or a list of pointers to the individual clinical events.

Failing legislation that provides for setting up the above framework in order to fulfil administrative obligations vested in Regions and/or central State bodies, the purposes that may be achieved by creating EHRs and/or HFs may only relate to the treatment of data subjects – i.e. affording the best treatment options to data subjects by building up as complete a picture as possible of the clinical events that have concerned the given individual over time, in connection with separate medical care activities/actions.

To safeguard data subjects, the purposes in question should accordingly only consist in prevention, diagnosis, care and rehabilitation of the given data subject and exclude any other objective – in particular planning, managing, supervising and assessing health care activities, which can actually be performed in several circumstances without using personal data. This is without prejudice to any requirements arising under criminal law.

If administrative purposes are to be also achieved via EHRs and/or the HF and such purposes are closely related to providing the medical care requested by the given data subject – e.g. as for booking and paying for a given medical examination – the tools in question should be organised in such a way as to keep administrative data separate from medical information. To that end, different authorisation profiles may be allocated as a function of the different operations to be performed.

Any future use of EHRs and/or HFs, in whole or in part, for further purposes related to scientific, epidemiological or statistical research should be compliant with sector-specific legislation and assessed specifically beforehand; this also applies to those cases – including a few EHR projects considered by our DPA – where the list of medical events concerning a given data subject is kept by a Regional organization.

3. Right to Create an Electronic Health Record and/or a Health File
Pursuant to Italy's Digital Administration Act (82/2005), it must be ensured that information is available, managed, accessed, transmitted, kept and used in a digital format with the help of information and communication technologies; compliance with the relevant data protection legislation and, in particular, the provisions contained in the Digital Administration Act is a prerequisite.

Additionally, to the knowledge of our DPA there is currently no piece of legislation whereby health care bodies are required to set up an EHR and/or a HF; accordingly, introducing either tool is a matter of discretion.

The purposes for which an EHR and/or a HF are set up mostly consist, as mentioned above, in documenting the "historical record" of medical events concerning a given individual, to enable perusal by the physician(s) treating that individual.

Since processing of the personal data via either EHRs or HFs is aimed at prevention, diagnosis, care and/or rehabilitation purposes, it must be compliant with the self-determination principle (section 75 et seq. of the DP Code). Every data subject must be in a position to freely decide whether an EHR/HF should be set up by including the medical information concerning them, or whether their medical records should only be available to the health care professional/body that treated them without being necessarily fed into EHRs and/or HFs.

Therefore, the right to create an Electronic Health Record and/or a Health File should translate into the assurance that everyone is free to decide, based on their consent, whether such records/files should be set up so as to include – as already pointed out – a wide gamut of medical information.

In order for the decision in question to be really free, any data subject that objects to the creation of an EHR/HF should in any case be afforded the treatments provided by the national health service without suffering negative consequences in terms of access to medical care.

The consent must be given on a separate, specific basis, even though it can come along with the one required in order to process personal data for health care purposes (see section 81 of the DP Code).

Given the purposes underlying establishment of an EHR/HF, suitable explanations should be provided to data subjects as for the usefulness of creating and making available as thorough a picture as possible of all the medical data concerning them in order to better support the health care body, the given physician and the data subjects themselves. In-depth knowledge of clinical information also relating to past events can actually facilitate spotting the items that are of help in assessing the given case.

However, "partitioning" of consent should be envisaged to enable data subjects to indicate their wishes – that is, there should be a general type of consent with a view to establishing the EHR plus the provision of specific consent to allow access to the EHR by the individual data controllers (e.g. general practitioners, paediatricians, pharmacists, hospital doctors.)

Whilst the usefulness of a thorough EHR/HF is undisputed, there should be the possibility not to include certain items of medical information in respect of individual clinical events – concerning, for instance, a given specialist medical examination and/or a given prescription. This also stems from the patient-doctor relationship, whereby the former can decide, after being duly informed, not to disclose certain events to the latter.

There should be the possibility to reverse this "blanking" of certain clinical events, whilst the implementing mechanisms should be such as to allow preventing any (or part of) of the entities authorised to access the data – at least initially – from automatically being informed of the circumstance that the given data subject has decided to "blank" the information in question (i.e. a mechanism to "blank the blanking" should be in place.)

Within this framework, a few EHR projects taken into consideration do empower data subjects to "blank" information via a "sealed electronic envelope", which is transparent and may only be opened, from time to time, with the data subject´s direct involvement; alternatively, random codes are allocated to individual events, which prevents establishing links between certain items of flagged information.

Where a data controller plans to set up an EHR/HF by also relying on medical data that concern

past clinical events (e.g. previous medical reports), that data controller should be authorised beforehand by the data subject, who should be empowered to exercise the "blanking" right mentioned above.

As for legally incapacitated persons, the consent in question should be given by the respective guardians and/or the person(s) exercising parental authority. The data subject´s consent should be obtained anew once he or she becomes of age (see sections 13 and 82(4) of the DP Code).

If consent is withdrawn – which is an option afforded by the law – the EHR/HF should not be implemented further. The medical records contained therein should be further available to the health care bodies that have drafted them (this applies, for instance, to the hospitalization information that may be used by the given hospital), without prejudice moreover to their retention where required under the law; however, they should no longer be shared among the other health care bodies/professionals treating the given data subject (section 22(5) of the DP Code).

If genetic data are processed in connection with an EHR/HF, the ad-hoc general authorisation issued by the Italian DPA will have to be complied with.

4. Entities Processing the Data

Processing of personal data via an EHR/HF is only aimed at prevention, diagnosis and treatment activities in respect of the data subject; accordingly, it should only be performed by health care practitioners – which does not include technical experts, insurance companies, employers, scientific associations and/or organizations, administrative bodies in the health care sector or otherwise, and the medical staff acting in their capacity as forensic medicine experts (e.g. when examining an individual to establish whether he or she is fit to work and/or drive).

As a rule, the data controller of the processing performed via an EHR/HF should be the health care body/organization as a whole where the medical records were drawn up – e.g. the health care unit, the given hospital, etc. (section 4(1)f. of the DP Code).

The data controller is empowered to appoint data processors; in any case, the data controller should appoint the natural persons that are in charge of the processing. Such persons may lawfully become apprised of the personal data that are processed via EHR/HF insofar as they abide by the tasks entrusted to them and follow appropriate written instructions (section 4(1)g. and h., and sections 29-30 of the DP Code).

The natural persons that are authorised to access an EHR/HF should be adequately informed about the specific arrangements applying to creation and use of such tools.

When appointing the persons in charge of the processing, the data controller/data processor should clearly specify who is authorised to perform which processing operations; in particular, suitable distinctions should be drawn between administrative staff and health care staff. It should also be specified whether the persons in question may only access the given EHR/HF or also make amendments and/or additions thereto (see point 5 below).

5. Which Data May Be Processed and How to Access the Electronic Health Record and/or a Health File

The data controller should carefully consider which relevant, non-excessive, and indispensable data should be included in an EHR/HF by having regard to the specific prevention, diagnosis, treatment and/or rehabilitation requirements (see section 11(1)d. and

section 22(5) of the DP Code).

Accordingly, priority should be given to solutions that allow modules to be set up so as to restrict access by authorised entities to the information – i.e., the data module – that is indispensable.

Based on a few EHR projects taken into consideration, this modular approach allows, for instance, selecting the health care information that can be accessed by the individual data controller authorised to access the EHR as a function of the respective sector of practice – e.g. in the case of an oncology network made up of operational units specialising in cancer treatment. This would ensure that only the information related to the given disease can be accessed.

Similarly, a few categories of practitioner such as pharmacists – who provide their services at a given stage in the treatment process – may only access such data (or data modules) as are indispensable to administer drugs – e.g. their access may be restricted to the list of drugs previously prescribed to the given patient so as to establish incompatibility between over-the-counter drugs and other drugs taken by the patient.

In some HF projects, the health care manager is in charge for assessing whether the medical information generated by the various units/entities is indispensable with a view to allowing access; additionally, the manager should also decide whether the information concerning (past) clinical events may be accessed by the unit/entity that is treating the data subject by having regard to the type of medical intervention and the grounds underlying the specific access request.

When setting up an EHR/HF and determining the information categories that should be included therein, also at a later stage, a data controller should comply with the legislation protecting anonymity of individuals – such as that protecting the victims of rape and/or paedophilia (Act no. 66 dated 15 February 1996; Act no. 269 dated 3 August 1998; Act no. 38 dated 6 February 2006); HIV-positive individuals (Act no. 135 dated 5 June 1990); individuals addicted to drugs, psychotropic substances and/or alcohol (Presidential decree no. 309 dated 9 October 1990); women undergoing abortion and/or deciding to give birth anonymously (Act no. 194 dated 22 May 1978; Ministerial decree no. 349 dated 16 July 2001); and the legislation on family advisory services (Act no. 405 dated 29 July 1975).

In most EHR/HF projects taken into consideration, compliance with the anonymity and confidentiality safeguards laid down in the above pieces of legislation was ensured, for instance, by requiring that the information related to the said clinical events should not be recorded within the given EHR/HF.

Some of the EHR/HF projects envisaged the drawing up of a summary of relevant patient clinical information, or else a set of information whose knowledge may prove indispensable to protect the data subject´s life (e.g. chronic disease, allergy reactions, use of life-saving drugs and/or devices, information on the use of prostheses and/or past transplantations). This information is contained, as a rule, in a separate module and can be accessed by all the entities providing health care; this circumstance should be made known to the data subject via the information notice mentioned in section 13 of the DP Code.

Furthermore, arrangements should be made to enable modular access to the EHR/HF in terms of the personal data at issue and the entities authorised to access such data – so as to ensure the self-determination right.

It should be specified clearly who is authorised to access and browse an EHR/HR. Given the purposes underlying creation of an EHR/HR, access should only be allowed for the purposes of prevention, diagnosis, and treatment of the data subject; only health care practitioners should be enabled to access the data – which does not include technical experts, insurance companies,

employers, scientific associations and/or organizations, administrative bodies in the health care sector or otherwise, and any medical staff acting in their capacity as forensic medicine experts.

The administrative staff working in a health care body where an EHR/HF is used should only access the information required to discharge the respective administrative tasks, and the information should be closely related to the specific service provided – for instance, the staff giving medical appointments for specialist visits and/or examinations should only access the data that are indispensable to make the given appointment.

Access by data subjects should be enabled in compliance with the precautions set forth in section 84 of the DP Code, whereby health care practitioners and bodies may communicate health status information to the data subject (e.g. medical reports, outcome of medical examinations) by the agency either of a physician – to be appointed by the data subject and/or the data controller – or of a health care practitioner that has direct contacts with the patient in the course of discharging the respective tasks. This precaution should also be complied with if the EHR/HF is accessed by means of a smart card.

Who drew up any record included in an EHR/HF as well as any entity treating the data subject should be allowed to access the EHR/HF, providing the data subject has authorised access in the manner specified above. In a few HF projects, access by certain categories (e.g. medical specialists) is authorised from time to time by the data subject via delivery of a smart card.

The health care professional / body that is treating the data subject should be enabled to access the EHR/HF by browsing the medical records they drew up and/or any records related to other clinical events as drawn up by other units and/or facilities that are part of the given data controller (as for the HF) or else by other health care bodies and/or practitioners (as for the EHR). This applies, for instance, to previous hospitalizations or clinical lab tests.

In any case, access to an EHR/HF should be allowed for no longer than is indispensable in order to carry out the treatment the given access-enabled entity is authorised to perform. Accordingly, the access-enabled entities should only be allowed to access such records/files as relate to the patients/data subjects they are treating throughout the duration of the treatment procedure the patient/data subject is undergoing.

The data controller will have to draw up and update an exhaustive list of the types of information falling within the scope of the so-called emergency data.

The legislation on access to administrative records (Act no. 241 dated 7 August 1990 as subsequently amended and supplemented) is obviously left unprejudiced.

6. Information Notice

To enable data subjects to make informed decisions, the data controller is required to provide a suitable information notice beforehand (sections 13, 79 and 80 of the DP Code).

The information notice should be worded clearly and contain all the items specified in section 13 of the DP Code. In particular, it should be highlighted that as complete an EHR/HF as possible would be set up to document the data subject's clinical history so as to improve treatment – i.e. for purposes of prevention, diagnosis, treatment and rehabilitation (see section 76(1)a. of the DP Code). The opportunities afforded by the EHR/HF should be clarified along with their possibly wide-ranging scope.

As already pointed out, the data subject should be informed that access to the required medical care will in no way be affected by their failure to consent, in whole or in part, to the processing in

question. This is necessary to safeguard the right to decide on whether an EHR/HF should be set up or not.

The information notice should clearly specify – in concise though easily understandable wording – the entities (or categories of entities) that, when treating the data subject, may access the EHR/HF as well as the possibility for the data subject to only allow part of those entities to access the EHR/HF. In the HF case, the notice should mention entities such as physicians working in the unit where the data subject is hospitalised and/or in emergency units; in the EHR case, the notice should mention the categories of entities other than the data controller (e.g. general practitioner, pharmacists, etc.).

As for the EHR, the information notice and the related consent could be provided on a separate basis in respect of the individual data controllers; it would be preferable to have a single information notice and consent declaration, whereupon the scope of the processing should be specified clearly in respect of the individual EHR participants.

The data subject should also be informed that the EHR/HF might be accessed – without their consent, albeit in compliance with the Italian DPA´s relevant general authorisation – if this is found to be indispensable to protect a third party´s and/or the public health (section 76 of the DP Code).

The information notice should also highlight that in allowing a given entity (e.g. a general practitioner and/or a medical doctor in the hospital unit where the data subject is hospitalized) to access the EHR/HF one is also allowing access by the respective locum tenens.

The information notice should also specify how data subjects can apply to the data controller in order to exercise the rights set forth in section 7 et seq. of the DP Code (see point 10 below) and/or withdraw their consent to implementation of the EHR/HF and/or exercise their rights to have certain clinical events blanked (see point 3 above).

To ensure that the information is fully understandable, the data controller should adequately train the staff concerned in the relevant data protection issues – also in order to enhance the relationships with data subjects.

7. Security Measures

Given the sensitiveness of the personal data processed via an EHR/HF, specific technical arrangements should be made in order to ensure the appropriate security level (section 31 of the DP Code) – without prejudice to the minimum measures data controllers are required to take in any case pursuant to the Code (section 33 et seq.).

If data storage/filing systems are used, suitable arrangements should be made to protect the data against unauthorised access to and theft and/or loss, in whole or in part, of the storage media and/or fixed/portable processing devices; to that end, encryption technologies might be applied to file systems and/or databases, or other protection measures might be implemented to prevent the data from being intelligible to unauthorised entities.

The following measures should also be taken:

- suitable authentication and authorisation systems should be applied to the persons in charge for the processing as a function of the respective access/processing requirements (e.g. as for browsing, changing and adding records);

- procedures should be in place to regularly check quality and consistency of authentication

credentials and authorisation profiles applying to the persons in charge for the processing;

- criteria should be laid down to encrypt and/or keep separate the data suitable for disclosing health and sex life from any other personal data;

- accesses and operations should be logged;

- audit logging should be in place to control database accesses and detect abnormalities.

As for EHRs, secure communication protocols should be deployed by implementing encryption standards for electronic data communications between the various data controllers.

8. Notification to the Italian DPA

The EHR is a logical set of health care information and records that is aimed at documenting a person's clinical history and can be shared by several data controllers; accordingly, it should feature top-level transparency both in terms of its structure and in terms of its operation. Hence, the processing operations of personal data performed via an EHR should be notified to the Italian DPA; the notification should be given by the public and/or private organizations involved rather than by the individual medical practitioners/professionals browsing the EHR (section 37 of the DP Code).

Pursuant to the DP Code, the Italian DPA is actually empowered to determine additional processing operations – other than those listed in section 37 – that should be notified insofar as they may be prejudicial to the data subject's rights and freedoms either because of the relevant mechanisms or on account of the personal data that are processed (see section 37(2) of the DP Code). The highly sensitive nature of the information processed in an EHR and the possibility for several data controllers to use that information would point to the need for notifying the processing in question to the Italian DPA in advance. Accordingly, the Italian DPA reserves the right to provide, following the public consultation, that EHR-related processing operations should be notified, in whole or in part.

9. Data Dissemination and Cross-Border Data Flows

The medical information contained in an EHR/HF may not be disseminated. Unfettered circulation of any information suitable for disclosing health is expressly prohibited by the DP Code – see section 22(8) and section 23(5) thereof. Any violation of the said prohibition gives rise to unlawful processing of personal data and carries criminal punishments (section 167 of the DP Code).

The medical data contained in an EHR/HF may only be transferred abroad for purposes of prevention, diagnosis and treatment in respect of the data subject if the data subject consents thereto – unless the transfer is necessary to safeguard a third party's life or physical integrity (section 43 of the DP Code). It is no chance that – if one considers the projects assessed so far – the data subject's medical information contained in an EHR/HF happens to be transferred abroad mostly to enable the data subject to undergo medical treatment and/or seek medical advice abroad.

10. Data Subject's Rights

Exercise of the rights set forth in section 7 of the DP Code should be allowed at any time

with regard to the personal data processed via an EHR/HF. The rights in question include the right to access the data and obtain their intelligible communication as well as the right to have the data supplemented, updated and/or rectified; they should be exercised by applying directly to the individual health care bodies/professionals.

The requests lodged by a data subject should be handled without delay, in full and in depth (see sections 7-10 and section 146 of the DP Code).

In particular, access requests should be complied with by extracting the requested information and communicating such information to the data subject in a manner that should make it easier to understand – where appropriate, the information should be made available on paper and/or magnetic media. The requests in question may only be rejected in the cases specified by the DP Code (section 8). Considering that medical records are at issue, any requests to have data supplemented, updated and/or rectified could be complied with by adding a note to the records with the requested changes, i.e. the original records need not be amended – similarly to what has been provided for by the Italian DPA concerning medical, bio-medical and epidemiological research activities.