EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The use of it tools and artificial intelligence in the health sector: the patient as a vulnerable subject

FABRIZIA ROSA
Ph.D. Candidate at University Parthenope of Naples

Abstract

The present work aims at analyzing the development of technologies in the healthcare sector and the impact this has had on patients' right to privacy.

After having examined the meaning of "digital health", it focuses on the main tools used nowadays for the processing of patients' data (telemedicine, electronic medical records and electronic health records) and on the risks they entail for the protection of patients' right to privacy.

Notably, since the processing of data includes personal and health data stored digitally, these are exposed to the possibility to be lost or become inaccessible, violated or stolen, circumstances that can lead to problems both on the individual level regarding privacy violation, and at the collective level, for example impeding the provision of health services.

In conclusion, in order to minimize these risks it is necessary that digitalization in the health sector become an organic and safe process and that health data management strategies are envisaged to ensure the protection and availability of data in a reliable and timely manner.

Keywords: health - patient - technologies - privacy.

Summary: 1. The patient and his rights: in particular, the right to privacy and the processing of health data. – 2. The processing of patient data in the emergency context by Covid-19. – 3. The development of healthcare technologies: some examples of digital healthcare. – 4. Digital healthcare at the time of Covid-19. In particular, the innovations introduced with reference to the *Fascicolo Sanitario Elettronico* (FSE or Electronic Health Records). – 5. The benefits and risks of digital health. In particular, the impact of new technologies on the processing of health data. – 6. The challenges that digital health poses and the perspectives *de iure condendo*.

1. The patient and his rights: in particular, the right to privacy and the processing of health data. Brief reference to the implications in the current emergency context.

The health care relationship that is established between the healthcare facility and the patient includes a complexity and heterogeneity of services that cannot be easily determined in advance. In particular, it is characterized by considerable accessory services and organizational duties of the structure, with the consequence that it would not be sufficient to speak only of a medical-surgical service in the strict sense, but, at most, of an atypical *ad hoc* contract. For this reason, doctrine[1] and jurisprudence[2] have coined the atypical contract

[1] P Stanzone, V Zambrano, *Attività sanitaria e responsabilità civile* (Giuffrè, 1998), 505 ff.; M Toscano, 'Il difetto di organizzazione: una nuova ipotesi di responsabilità? (note to Court of Monza June 7 1995)' (1996) Resp. civ. e prev., 389 ff.

[2] In this sense, after several pronouncements from the jurisprudence of merit, the United Sections of Court of Cassation of 2002 were expressed, according to which '*The complex and atypical relationship that is established between the clinic and the patient (in this case: a pregnant woman), even if the latter chooses a treating doctor from outside the health care*

of expediency, to which the ordinary rules on non-performance established by art. 1218 apply. In particular, this term is intended to indicate the complex synallagmatic contract with corresponding services between the health facility and the patient, which includes - at the expense of the former - a whole series of services, additional to medical and / or surgical assistance, which consist, among others, in duties of management of medical and paramedical personnel, maintenance of machinery and premises of the structure, guarantee of maintenance of sanitary conditions necessary for the use of services, supervision and control of instruments and pharmaceutical products used and so on.[3]

Faced with all the above mentioned duties of the hospital, there are a series of rights due to the patient as such, to know about which it is essential to keep in mind the European Charter of Patients' Rights issued in 2002, which is a key reference point for all health care professionals, as well as for patients.

In particular, these include the right to information (the patient has the right to know all information regarding his or her state of health, the health services that can be used and how to access them); the right to consent (the patient has the right to know all useful information in order to be able to consent to the treatment he or she undergoes); the right to free choice (the patient, properly informed, has the right to choose freely between the various possible forms of treatment); the right to respect time limits (the patient has the right for each phase of treatment to receive treatment in a short and predetermined time); the right to respect quality standards (the patient has the right to high quality treatment); the right to safety (the patient has the right not to suffer damage from medical errors or malfunction of equipment and/or health services) and so on.

But the right we focus on here is the right to privacy: the citizen who comes into contact with health facilities for diagnosis, treatment, medical services, administrative operations and other, must be guaranteed the most absolute confidentiality and the widest respect of his or her fundamental rights and dignity.

As is well known, privacy is a set of rules created to ensure that the processing of personal data is carried out with respect for the fundamental rights and freedoms of everyone.

In the health sector, however, given the delicacy of the data processed and the position of the parties involved, the processing of personal data receives a specific discipline.

Before the entry into force of EU Regulation 2016/679 (c.d. GDPR: General Data

---

facility, is not limited to the mere provision of services of a hospitality nature (provision of board and lodging), but consists in the provision of auxiliary medical and paramedical personnel and the provision of medicines and all necessary equipment, even in view of any complications', Court of Cassation, United Sections, 1 July 2002, n. 9556, in Giust. civ., (2003), 2196.

This decision has then been followed by other pronouncements of the simple sections: see, in such sense, Court of Cassation, 3rd Civil Section, 13 January 2005, n. 571, in *Danno e resp.* (2005), 5, 563, which states the following principle: "*The relationship that is established between patient and private nursing home (or hospital institution) has its source in an atypical contract with protective effects on the third party, from which, against the obligation to pay consideration (which can well be fulfilled by the patient, the insurer, the national health service or another body) arise at the expense of the nursing home (or institution), in addition to those of broadly hospitality nature, obligations to make available auxiliary medical personnel, paramedical staff and the provision of all necessary equipment, including in view of any complications or emergencies. It follows that the responsibility of the nursing home (or the institution) towards the patient has a contractual nature, and may result, pursuant to art. 1218 of the Italian Civil Code, in the non-fulfillment of the obligations directly in its charge, as well as, pursuant to art. 1228 of the Italian Civil Code, the non-fulfilment of the medical-professional service provided directly by the health care professional, as his necessary auxiliary, even in the absence of a subordinate employment relationship, however, since there is a connection between the service provided by him and his company organization, not noting, on the contrary, the fact that the health care professional is also "trusted" by the same patient, or in any case by the same one*"; Court of Cassation, 3rd Civil section, 26 January 2006, no. 1698, in Mass. Giur. it., (2006); Court of Cassation, 3rd Civil section, 13 April 2007, n. 8826, in Mass. Giur. it. (2007).

[3] It is on the basis of these duties that the minimum requirements that a health facility must meet have been articulated.

Protection Regulation)[4], with particular reference to the processing of health data, the former Privacy Code (Legislative Decree 196/2003) provided that the same could be processed only with the consent of the person concerned and after authorization from the Guarantor (art. 26, paragraph 1). In other words, the consent of the interested party was given a central role as a legitimate prerequisite and condition of lawfulness of the processing of personal data. Therefore, the rule was that the personal data could be processed only with the consent of the person concerned and exceptions were provided for (and justified) only by the extraordinary nature of certain situations.

However, there were a number of cases in which the processing of health data was allowed even without consent, without prejudice to the need for prior authorization from the Guarantor. In particular, reference was made to the case in which the processing of data was *necessary* to safeguard the life or safety of a *third party*. If, on the other hand, the same need arose with reference to the person concerned and he or she was unable to give consent due to physical impossibility, inability to act or inability to understand and want, it was provided that the same was "manifested by those who exercise legal power, or by a close relative, a family member, a cohabitant or, in their absence, by the manager of the facility where the person concerned resides".

Similarly, art. 82 of the Privacy Code took into account emergency situations, providing that the information and consent to the processing of personal data could intervene "without delay, after the performance [of medical services]", when there was one of the following hypotheses: a) physical impossibility, incapacibility of giving consent of the person concerned, when it is not possible to obtain consent from the persons indicated in letter b) of art. 26; b) serious, imminent and irreparable risk for the health or physical safety of the person concerned; c) medical performance that may be affected by the prior acquisition of consent, in terms of timeliness or effectiveness.

From the combined reading of these articles, it emerged that, in fact, in the codicistic system there were no cases in which the processing of health data for the purposes of treatment of the person concerned could disregard the granting of consent (prior or subsequent, directly from the person concerned or from a third party, but always present and necessary).

Moreover, the previous system did not provide for the hypothesis in which the interested party, while requesting a health service necessary for the protection of her life or physical safety, could refuse to give consent to the processing of her personal data. According to the Code, in such a case, the doctor should have refused to provide the service.

Another unforeseen hypothesis was the one in which, since one of the hypotheses referred to in art. 82 existed, the doctor had already performed the service without requesting consent and subsequently the person concerned had refused to grant it. Here, a doctor that intervened promptly to safeguard the safety of the person concerned would have risked being called to answer for having illegally processed the patient's personal data.

In conclusion, the previous regulatory system provided that the processing of health data could only take place with the consent of the person concerned, except in exceptional cases.

However, it soon became clear that consent was inadequate as a legal basis for the processing of health data.

In this regard, the GDPR (EU Regulation 2016/679) intervened, overcoming the previous approach and introducing a new one for the management of personal data processing in the health sector.

[4] EU Regulation 2016/679 came into force on May 24, 2016, but has been applied in EU States since May 25, 2018. In Italy, the GDPR was implemented by Legislative Decree no. 101/2018, which came into force on September 19, 2018.

With EU Regulation 679/2016, in fact, the centrality of consent has disappeared, in the sense that it is only one of the possible alternatives (or rather, legal bases) on which the processing of personal data can be founded, placing itself on the same level with respect to the other 5 legitimizing assumptions - all abstractly suitable to constitute a condition of lawfulness for the processing of data.

The lack of the centrality of consent is even more evident with reference to the processing of special categories of personal data, such as those "*related to health*", which, among other things, find for the first time in the GDPR their specific definition: they are "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*" (art. 4 GDPR).

In fact, unlike in the past, the health professional no longer has to request the patient's consent for treatment regarding essential services (clearly, this refers only to the treatment necessary to achieve the specific "treatment purposes" provided by the GDPR itself, and not also to those carried out for different purposes, such as promotional, commercial and so on).

But let's go in order.

The new configuration of the Regulation is based on the combined provisions of art. 6 and art. 9 dedicated to the "*Processing of special categories of personal data*".

First of all, since "health-related data" are included among the special categories of personal data, which, by their nature, are particularly sensitive and, therefore, need a higher level of protection, they are subject to the general prohibition of processing (art. 9, par. 1); secondly, the prohibition, derogated from the following par. 2 which allows the processing of the same provided that at least one of the ten conditions listed therein is met. In particular, for the health sector, the conditions set forth in letters g), h) and i) are relevant[5].

Letter g) refers to the hypothesis of relevant public interest on the basis of EU law or Member States; letter h) refers to treatment purposes, i.e. preventive medicine, diagnosis, health or social care or therapy or management of health or social systems and services on the basis of EU or Member State law or in accordance with the contract with a health professional (see also par. 3 of the GDPR and recital no. 53); letter i) refers to hypothetical cases of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products and medical devices, on the basis of Union or Member State law providing for appropriate and specific measures to protect the rights and freedoms of the person concerned, in particular professional secrecy (see also recital 54) (e.g. health emergencies following earthquakes and food safety).

Moreover, the possibility for national legislators to introduce stricter conditions, aimed at ensuring a higher level of protection than that resulting from the Regulation (art. 9, par. 4), remains unchanged.

In any case, from May 25, 2018 (date of definitive applicability of the GDPR), the existence of the assumptions provided by letters g), h) and i) will be sufficient conditions to allow the processing of the health data of patients, without the need to acquire their consent.

Once the existence of one (or more) of the above conditions has been ascertained, the general prohibition of processing as per paragraph 1 of art. 9 will be lifted, with the consequence that health data can be processed, similarly to the "ordinary" categories of personal data, referring to one of the legal bases as per art. 6.

Art. 6, in fact, in regulating the lawfulness of the processing, lists six different legal bases among which the data controller, consistently with the principle of accountability, must identify the most appropriate one at any given moment. In this list, the consent of the person

[5] In this regard, see Gruppo di lavoro Bioetica COVID-19, 'Protezione dei dati personali nell'emergenza Covid-19', Rapporto ISS COVID-19 No. 42/2020 (2020), version of May 28, 3.

concerned appears only as one of the possible alternatives on which the processing of personal data can be based and is on the same level as the other legitimate assumptions.

However, since, as previously stated, consent cannot constitute a valid legal basis for the processing of personal data necessary for the provision of health services (since, to repeat, failure to do so would make it impossible to receive the requested service), a different legal basis must be identified.

The second step, therefore, consists in identifying the most appropriate legal basis for such processing, which once identified, will make it possible to process data relating to health.

Therefore, there is no longer a relationship as a rule - exception, but rather a plurality of equal conditions are identified.

In fact, the doctrine[6] is now in agreement in affirming that the Regulation has equalized the consent of the interested party to any other legitimate basis provided by law: "*These are conditions that are equivalent to each other and equal in order, it being sufficient that there is at least one that is able to consider the first stage of the evaluation process as regards the lawfulness of the processing to be passed*"[7].

Once the approach outlined by the GDPR has been defined, it is appropriate to consider how this is coordinated with the Italian regulatory system.

In Italy, on 19 September 2018, Legislative Decree no. 101 of 10 August 2018, containing provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 (so-called adaptation decree), came into force.

This decree confirmed the approach of the Regulation with reference to both the six legal bases of the processing and the ten conditions for the processing of special categories of personal data, thus confirming the possibility of processing data relating to health even without the consent of the person concerned. Of particular importance was the repeal of art. 81 concerning the "*Provision of consent*", which provided for the possibility to express orally the consent to the processing of data suitable to reveal the state of health, with annotation of the health professional for the purpose of documenting the granting of consent. This abrogation, in a rather clear-cut way, confirms the disappearance of the need to acquire the patient's consent and, among others, demonstrates the legislator's intentions to fully adapt the national regulations to the Regulation, overcoming, also with reference to health data, the previous concept based on the centrality of consent.

In any case, regardless of the decree of adaptation, as of May 25, 2018 the Regulation is definitively applicable in all Member States, with automatic disapplication of all national rules incompatible with it.

Consequently, from that date, even in the absence of the adjustment decree, it has become possible to process health-related data for medical purposes without the need to obtain the consent of the person concerned, provided that one of the conditions set forth in paragraph 2 of Art. 9 of the GDPR is met and the processing is based on one of the legal bases set forth in paragraph 1 of Art. 6 of the GDPR.

---

[6] See L Lipari, 'Privacy: dal Regolamento (UE) 2016/679 al d.lgs. n.101/2018' (2019), 7 February, diritto.it: '*the failure to give consent when data are processed for diagnosis and treatment (art. 2-septies of the Privacy Code amended by Legislative Decree no. 101/2018 in combination with art.9 GDPR)*' would represent the transition '*from a consensus-centric system to a system where it is necessary to first ask oneself and understand the reasons why the data are processed, and then evaluate, in light of the identified purpose, the basis of lawfulness of such processing*'. Available at https://www.diritto.it/privacy-dal-regolamento-ue-2016-679-al-d-lgs-n-101-2018/. On this point, see also G Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli 2017) 101 ff.; and L Bolognini - E Pelino – C Bistolfi, *Il Regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali* (Giuffrè 2016) 277 ff.

[7] G Finocchiaro, *Il nuovo Regolamento europeo sulla privacy,* (n 6) 126.

2. The processing of patient data in the emergency context by Covid-19.

The treatment of health data in the current emergency context of the Covid-19 pandemic merits a brief, but necessary, mention.

Given what has been said in the previous paragraph - that is, that art. 9 par. 2 GDPR lists the exceptions to the general prohibition of processing "special categories of data", including those on health, making them lawful to process, in particular when of interest to letters g), h), i) - it must, first of all, be emphasized that in a situation such as the one in which we, unfortunately, still find ourselves, the data processing activity falls within the hypothesis provided by art. 9 par. 2 letter i) of the GDPR which, to reiterate, allows the processing of health data when it "is necessary for reasons of public interest in the public health sector".

It is no coincidence that decree-law no. 14 of March 9, 2020, containing urgent provisions for the strengthening of the National Health Service in relation to the emergency of COVID-19 (published in Gazzetta Ufficiale no. 62, on March 9, 2020, and in force from March 10, 2020) allows a simplified regulation for the protection of personal data based, in fact, on art. 9 par. 2 letter i) of the Regulation[8].

In particular, the aforementioned Legislative Decree no. 14/2020, emphasizes that the simplified rules for the protection of personal data in the health emergency - which are temporary in the sense that they are intended to have a duration no longer than the duration of the state of emergency - are designed to make the exchange of information between health authorities easier and faster, as well as speed up and streamline the process of clinical trials of new medicines, protocols and medical devices; in addition, the increase in the archiving potential of patient information makes the entire system of management of the current health crisis more fluid and effective.[9]

Also of interest, we should highlight the need, emergent from the current emergency context, to properly manage personal data related to health that may be useful for scientific research and statistical data collection.

Given the sensitivity of the issue and the data processed, on April 21, the EDPB (European Data Protection Board) intervened on the issue by adopting specific "Guidelines" on the processing of health data for scientific research purposes in the context of the Covid-19 emergency, aimed at addressing the fundamental legal aspects of the case. The EDPB clarifies that the GDPR already contains numerous provisions on the processing of health data for scientific research purposes, which also apply in the context of the pandemic[10]. In addition, the document recalls that it is still necessary to respect the principles provided by Article 5 of the GDPR, including, in more detail: transparency; purpose limitation; data minimization and storage limits; integrity and confidentiality.

Subsequently, at the national level, the Guarantor for the Protection of Personal Data intervened on this point and, having examined the EDPB "Guidelines", dedicated a section of the FAQ on Covid-19 to "Data processing in the context of clinical trials and medical research in the context of the Covid-19 health emergency".

In particular, the legal bases that are indicated necessary so that, in the current emergency context, the processing of this particular category of personal data may be considered lawful are (alternatively): (i) the consent of the patient (art. 9 par. 2 letter a); (ii) the reasons of relevant public interest (art. 9, par. 2, letter g) GDPR); reasons of public interest in the field of public health (art. 9, par. 2. letter i); purposes of archiving in the public interest, scientific or historical research or statistical purposes in accordance with article 89, paragraph 1 (art. 9

---

[8] See Gruppo di lavoro Bioetica COVID-19, "*Protezione dei dati personali nell'emergenza Covid-19*", (n 5), 8.
[9] G Resta, 'La protezione dei dati personali nel diritto dell'emergenza Covid-19' (2020), 5 May, Giustiziacivile.it,.
[10] For example art. 5, par. 1, lett. b) and lett. e); art. 14, par. 5, lett. b); and art. 17, par. 3, lett. d) GDPR.

par. 2 letter j).

The National Guarantor for the Protection of Personal Data in its analysis also pointed out that the issue of processing necessary for reasons of relevant public interest (Article 9, paragraph 2, letter g) GDPR) could have created difficulties at this specific time and, therefore, deemed it necessary to introduce exceptions.

This is because it is precisely the public interest and public health that, in this particular period of health emergency, risk being in conflict with the interests and the right to the protection of personal data of patients affected by COVID-19, who witness the use of their data for the diagnosis and treatment of the disease, for scientific research and for statistical purposes. Therefore, the need to balance the interest of the protection of personal data and the interest of the protection of public security (*rectius*, health) emerges in all its scope.

Creating difficulties in this balance were in particular the provisions of art. 110 of the Privacy Code (Legislative Decree no. 196/2003 amended by Legislative Decree no. 101/2018), which contain the actual content of art. 9 par. 2 letter j) GDPR in conjunction with art. 6 par. 1 letter. f) providing that "*The consent of the interested party for the processing of data relating to health, for the purposes of scientific research in the medical, biomedical or epidemiological field, is not necessary when the research is carried out in accordance with provisions of law or regulation or European Union law in accordance with Article 9, paragraph 2, letter j) of the Regulation, including the case where the research is part of a biomedical or health research program provided under Article 12-bis of Legislative Decree no. 30 December 1992. 502, and an impact assessment is conducted and made public pursuant to articles 35 and 36 of the Regulation*".

Art. 110 continues with "*consent is also not necessary when, due to particular reasons, informing the interested parties is impossible or involves a disproportionate effort, or is likely to make it impossible or seriously jeopardize the achievement of the objectives of the research. In such cases, the data controller adopts appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, the research program is subject to a reasoned favourable opinion of the competent ethics committee at territorial level and must be submitted for prior consultation with the Guarantor*".

These provisions and requirements would have risked blocking the collection of data to carry out the research necessary to counter the epidemiological crisis of COVID-19 and, such blocking, could clearly not be permitted to occur. Hence the decision to intervene with FAQ, introducing a derogation, albeit partial, to art. 110 in cases of data processing concerning experimental studies and compassionate uses of medicinal products for human use for the treatment and prevention of the virus, establishing that "*holders who intend to carry out processing of personal data relating exclusively to experimental studies and compassionate uses of medicinal products for human use, for the treatment and prevention of the Covid-19 virus, are not obliged, under the legislation relating to this emergency phase, to prior submission of the research project, or of the related impact assessment or to submit the prior consultation of the Guarantor referred to in art. 110 of the Privacy Code*".

Therefore, despite the fact that European and national legislation on the processing of personal data applies also in this particular emergency phase, the need has emerged to adapt this legislation to the necessity to collect data from patients affected by COVID-19 for scientific research purposes, in order to find the medicines and treatments suitable for the treatment of this new virus, striking a balance between the rights of the patient concerned, which are partially limited, and the public interest in health protection[11].

From what has been said so far - given the close connection between personal confidentiality and public safety - the need to give priority to collective safety (and health) over the protection of individual health data has clearly emerged.

In the face of this, however, it must be stressed that, if it is true that in emergency

[11] V Lemma, 'COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico' (2020), 8 June, osservatoriomalattie.rare.it.

situations the right to the protection of personal data must be balanced with higher-ranking rights (such as the right to safety and public security), this does not mean that the same can be arbitrarily compromised[12]. In fact, any of its limitations must respect the canons of reasonableness and proportionality[13] and cannot go so far as to affect the essential content of the law itself, since it can never (and must never) involve the integral sacrifice of the intangible core of the fundamental rights of the human person.

In this sense, finally, the jurisprudence of the European Courts has intervened, which has helped to define the impassable stakes and the minimum or essential content of the right to data protection, recalling the principles of proportionality and strict necessity of the limitations concretely adopted[14].

3. The development of technologies in the health sector: some examples of digital healthcare.

Having provided a premise about the meaning of "health data" and the processing of health data, we now move on to analyse what the impact of the development of technologies in the health sector has been and what problems have arisen, particularly with regard to the patient's right to privacy.

New technologies and, in particular, the digitization of information - with the possibility of its sharing and use granted by the Internet - have created new forms of cultural, professional and organizational interaction in the health sector and have had repercussions on the traditional way of managing health and illness, with respect to the doctor-patient relational approach and related medical-legal aspects.

With current technologies, examinations are faster, diagnoses more accurate and all information, images, reports and consultations can "travel" digitally. Thanks to an internet network capable of supporting high data flows, it is possible to monitor and manage patients through systems that allow ready access to their clinical profiles even remotely, a possible

---

12 See in this regard F Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali* (Giappichelli, 2016) 21. See also B Caravita, 'L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana' (2020), 6, Federalismi.it; L Panzani, 'COVID-19. Un'emergenza destinata a protrarsi. Appunti per il "dopo"' (2020), 10, Federalismi.it; M Tresca, 'Le fonti dell'emergenza. L'immunità dell'ordinamento al covid-19' (2020), 3, Osservatorio AIC; E Grosso, 'Legalità ed effettività nel tempo del diritto costituzionale dell'emergenza' (2020), 16, Federalismi.it; M Cartabia, 'Nella Costituzione le vie per uscire dalla crisi. Possibili limitazioni ai diritti ma proporzionate e a tempo' (2020), 29 April, interview in Corriere della sera, 9. See also G Resta, 'La protezione dei dati personali nel diritto dell'emergenza Covid-19' (n 9), in which the author refers to the "*right to human intervention*" in art. 22 GDPR, to be taken "*as the north star of a fruitful interaction between man and machine, aimed at the simultaneous realization of two fundamental rights, that of health and that of the dignity of the person*".

13 M Cartabia, 'Nella Costituzione le vie per uscire dalla crisi. Possibili limitazioni ai diritti ma proporzionate e a tempo' (2020), 29 April, interview on Corriere della sera, 9; M Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana', speech presented to: Incontro trilaterale tra la Corte costituzionale italiana, la Corte costituzionale spagnola e il Tribunale costituzionale portoghese, Rome, (2013); G Scaccia, Il principio di proporzionalità, in S Mangiameli (ed.), L'ordinamento europeo. L'esercizio delle competenze (vol. II, Giuffrè, 2006), 225-274.

14 Judgment of 9 November 2010, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, joined cases C-92/09 e C-93/09, EU:C:2010:662; Judgment of 8 April 2004, Digital Rights Ireland and Kärntner Landesregierung, joined cases C- 203/12 e C-594/12, EU:C:2014:238; Judgment of 21 December 2016, Tele2 Sverige, C-203/15, EU:C:2016:970; Judgment on the merits delivered by a Chamber, *Antović e Mirković v. Montenegro*, no. 70838/13, § 42, ECHR 2017; Judgment on the merits delivereb by Grand Chamber, *Bărbulescu c. Romania,* no. 61496/08, ECHR 2017

prescription of medical care and the use of expert advice, regardless of where they reside.[15]

Therefore, not only the clinical-assistance processes, but also those concerning the management of patient data are subject to great changes.

The biggest and most recent innovation in the healthcare field concerns the use of information technology and is dubbed e-Health[16]. The term generally refers to any exchange of health data, collected and analyzed with the help of electronic and computer technologies, to improve the effectiveness and efficiency of health care[17]. To simplify, "e-Health" refers to the way in which information and communication-based technologies support health-related areas.

Among the various tasks assigned to digital health are: (i) care; (ii) surveillance; (iii) studies to promote prevention and diagnosis; (iv) treatment and monitoring of patient conditions and so on. And, in order to achieve these goals and for the results to be as expected the most cutting edge (and increasingly so) technology and artificial intelligence tools are used today.

It is evident that the rapid development of technology in the healthcare field has radically changed, in recent years, (and is still changing) the practice of medicine and its future developments.

In this regard, it cannot be underestimated that, further spurred by the COVID-19 health emergency, digital healthcare is making important steps forward.

In fact, physicians are increasingly connected with patients through digital channels and artificial intelligence is showing its potential for customization of care. In this respect, the pandemic has been an opportunity to experiment with solutions aimed at containing contagion, reducing hospitalizations and managing patients in a given locality; but also to redesign new models of care by accelerating the transition to a more connected, sustainable and resilient healthcare model.

From this point of view, it can be said that medicine and technology are evolving towards a connected healthcare model, the so-called Connected Care.

In order to fully understand the extent of the impact of the development of technologies in health care, it seems appropriate to focus on some of the most widespread tools used today: telemedicine, electronic medical records (CCE) and electronic health records (FSE in Italy - *Fascicolo Sanitario Elettronico*).

Among the most direct new developments in the digitization of healthcare, there is, first of all, ***telemedicine***. The term is a neologism resulting from the composition of two words: telematics (i.e. the set of applications derived from the integration of information technologies with those of telecommunications, based on the exchange of data or access to archives through the telephone network or special networks) and medicine. As is evident, telemedicine involves three different scientific-disciplinary areas: telecommunications, information technology and medicine.

This tool, in fact, involves the use of telecommunications, as well as electronic and information technologies to support medicine when the patient is geographically separate from the medical staff. Appropriately, therefore, telemedicine is defined as "the remote use of medical expertise in the place where the need arises”[18].

---

15 M Zagra - S Zerbo - A Argo, ‘Informatica, web e telemedicina’, in M Zagra - A Argo – B Madea (ed.), *Problem-oriented forensic medicine* (Elsevier, 2011), 123 ff.

16 “‘eHealth” replaces the older term telemedicine’, WHO, Building Foundations for eHealth, Report of the WHO Global Observatory on eHealth, 2006, 2.

17 J P Harrison – A Lee, ‘The Rule of E-Health in Exchanging Health Care Environment’ (2006), 24(6), Nurs Econ., 284

18 This definition can be found in Telemedicine Glossary, Glossary of standards, concepts, technologies and users. European Commission Information Society Directorate-General - Unit B1 Applications relating to Health edited by Dg Infso- B1 version 2.10, May 2000. The value of this definition consists in highlighting the

Even more comprehensive is the definition approved at the EU level, for which telemedicine is "the integration, monitoring and management of patients, as well as the education of patients and staff, using systems that allow ready access to expert advice and patient information, regardless of where the patient or information resides" (AIM 1990)[19].

It is a digital tool that simplifies and improves healthcare procedures between doctors and patients, especially in monitoring health conditions.

Telemedicine, therefore, represents an innovative approach that reorganizes the health care network between doctor and patient, facilitating the provision of services at a distance by using digital devices.

Prevention, diagnosis, treatment and patient monitoring can be performed even without going to traditional health care facilities, with the advantage of simplifying and making the best care accessible to all through a secure exchange of information, images and documents between professionals and patients.

In the current context of the Covid-19 health emergency, telemedicine has intervened (and still intervenes) to manage emergency activities in a timely manner, exploiting the immediacy of digital technology to exchange clinical information in the health network and improving the management of critical or unreachable patients.

This tool, however - like those that will be examined below - presents some critical aspects, such as the protection of the right to patient confidentiality, which should not be underestimated, and which we will address shortly.

Another important tool is the ***electronic health record (EHR***, also known by its most commonly used brand acronym, CCE, provided by the technology company IBM), which is the digital evolution of the traditional medical record, i.e. in paper format[20].

It represents, therefore, an instrument to support clinical decision-making processes, as it is the manager of the complete history of the patient, both inpatient and outpatient, promoting the continuity of the latter's care through the archiving of all clinical episodes related to the same hospital structure.

It is an essential starting point to have the information related to the patient's clinical history as soon as possible, in order to achieve an overall improvement in the quality of care[21].

In other words, it is a "virtual file that contains the clinical records and past, present and

---

evolution of the concept of telemedicine from a mere "practice of medicine without the usual physical confrontation between doctor and patient, using an interactive multimedia communication system" (BIRD, 1975) to the use of the same to overcome the problem of spatial distance between doctor and patient. For a general overview of the phenomenon of telemedicine, see E Coiera, *Guida all'informatica medica, Internet e telemedicina* (Il Pensiero Scientifico, 1997).

[19] This definition, in addition to highlighting, like the previous one, the evolution of telemedicine in the sense of solving the problem of the physician-patient spatial distance, also focuses on the Anglo-Saxon concept of "telehealth", which brings with it a revolution in the health system, in all its aspects, from medical organization to the management of emergency services and health education in general. In this regard, it seems enlightening the definition that, already back in 1976, the Committee for Telemedicine created by the University of Rome gave telemedicine, seeing it as "*a global system of reorganization of health structures in which modern means of telecommunications constitute the backbone*".

[20] On the definition of "medical record", see A Rossi - R. Maceratini, 'La cartella clinica elettronica (Electronic Patient Record)', in R Maceratini - F Ricci (ed.), *Il medico online - Manuale di informatica medica* (Verduci Editore, 2000), chap. VI. The guidelines of the Ministry of Health of June 17, 1992 ("The compilation, coding and management of the hospital discharge form established ex D.M. 28.12.1991"), define the medical record as "*the individual information tool designed to detect all significant personal and clinical information relating to a patient and a single episode of hospitalization"*.

[21] G Cangelosi, 'I servizi pubblici sanitari: prospettive e problematiche della telemedicina' (2007) 1, Dir. fam. e pers., 440.

future information tied to the physical and mental health of the patient"[22].

At the international level, among the many existing definitions of "medical record", the most synthetic and effective one reads: *"The medical record is the who, what, why, when and how of patient care during hospitalization"*[23].

In conclusion, it is a digital document created by the healthcare facility that cares for the patient, which can also be shared with their family doctor and other specialists and which allows the complete dematerialization of the document production, with a management of information from a digitalized origin.

Finally, among the tools mentioned above, there is the ***electronic health record (FSE*** in Italy), which aims to provide health system operators with a global and unique vision of the health status of each citizen.

Established with Legislative Decree no. 179 of 2012, which defines it as "the set of digital data and documents of a health and sociomedical type generated by clinical events present and past, concerning the patient"[24], it represents the tool in which to bring together information and clinical documents of individual citizens generated in various ways by the national health service (SSN in Italy). It contains health events and documents summarized and organized according to a hierarchical structure, which allows to navigate through the documents in alternative ways depending on the type of investigation to be carried out.

Its introduction, in addition to streamlining the time-consuming processes dictated by the paper-based management of patient clinical information, leads to an improvement in the quality of services and significant cost containment.

Therefore, the FSE - unlike the electronic medical records, managed by the individual hospital - has the citizen as its center and was created to respond to the need for sharing clinical data and the principle of "interoperability" (on which, we will focus shortly).

4. Digital healthcare at the time of Covid-19. In particular, the innovations introduced with reference to the Electronic Health Record (FSE).

The usefulness and effectiveness of digital health tools (all, not only the FSE), where correctly and uniformly used, has emerged, in all its scope, in the current health emergency situation caused by Covid-19, which has highlighted two aspects: (i) the need to innovate and adapt these instruments to the current context and, therefore, to this situation's new needs, trying to ensure their linear and homogeneous use throughout the national territory; (ii) the need, increasingly felt, to find a solution to the risks that could arise from a distorted use of these digital health instruments, with particular attention to the protection of the patient's right to privacy.

With regard to the first aspect, it seems appropriate to dwell, in particular, on the relaunch of the Electronic Health Record (FSE), on whose discipline the Government wanted to propose important reforms in light of the recent experience gained in the pandemic by COVID-19.

Indeed, this instrument should have been activated in all regions and autonomous provinces by June 30, 2015, but, at the beginning of the pandemic, it was used in very few

---

[22] C Rabbito, 'La cartella clinica elettronica ed i suoi vincoli giuridici' (2007), June, Telemeditalia – Giornale di tecnologia medica, rubrica telesalute. The article highlights how the design of an eHealth system, which provides for the computerization of medical records, must necessarily take into account the particular nature of "public act" of the so-called "virtual file" and the consequent responsibilities (including criminal) of the various officials who will intervene on it in the insertion, modification and storage of health information.

[23]Source: American Hospital Medical Record Association

[24] Art. 12 of Legislative Decree no. 179 of October 18, 2012, on "*Further urgent measures for the growth of the country*" (converted, with modifications, from l. 17 December 2012, n. 221).

Italian regions and activated only by 20% of the population[25].

Therefore, in order to facilitate its use and encourage its activation, the legislator intervened by amending Article 12 of Legislative Decree No. 179 of 2012, through Article 11 "*Urgent measures on FSE*" of Decree-Law No. 34 of May 19, 2020 (the so-called "Relaunch" Decree), in particular, expanding the types of health data that must be fed into the FSE - making explicit reference to all digital health and sociomedical documents, referring to the services provided both by the National Health Service (SSN - *Servizio Sanitario Nazionale*) and outside the SSN - and, above all, widening the number of subjects qualified to feed the FSE, including, in addition to the patient with the medical data in their possession, also the health care professionals who take care of the patient both within the SSN and regional social and health services, and outside them. Therefore, there is also an opening of the FSE to private subjects whose systems will have to interact with the public standard and comply with the defined safety measures[26].

In addition, the decree eliminates the requirement of consent (free and informed) of the person concerned-assisted to the FSE (repeal of paragraph 3-bis of Art. 12 of Legislative Decree no. 179 of 2012); however, consent remains a condition *sine qua non* of the activation and consultation of its file.

The above changes made to the FSE offer many a food for thought.

In particular, as far as of interest here, there is to be considered that if, on the one hand, all these interventions lead to an increase in the use of the FSE, on the other hand one cannot but wonder if - in the face of an increase in data flows and subjects who will interact with the different FSE systems - the certainty of the origin and correctness of the data themselves can be fully guaranteed, as well as the accessibility of the same only by legitimate subjects[27].

And in fact, given that the task of making access to FSE information operational is the responsibility of the Regions - which must also promote interoperability throughout the national territory through the technical specifications published by the AgID (Agency for Digital Italy)[28] - cannot underestimate the fact that, to date, digital health is evolving discontinuously with respect to the different regional plans[29], and this does not always allow to meet the needs of interoperability and security[30].

Let's explain further. In the light of what is prescribed by the GDPR, the archiving system of documents present in the FSE is subject to the preparation of technical-organizational models and security measures aimed at ensuring the application of the European Regulation[31]

---

[25] See in this regard the monitoring activities divided into two distinct groups of indicators: Implementation and Use, available on the Agid website at the following link: https://www.fascicolosanitario.gov.it/monitoraggi.

[26] See Gruppo di lavoro Bioetica COVID-19, 'Protezione dei dati personali nell'emergenza Covid-19' (n 5), 15.

[27] A Fiaschi, 'Fascicolo Sanitario Elettronico: i rischi per la data protection delle politiche di sanità integrata' (2020), 28 January, *Cybersecurity.it.*

[28] For the specifications you can consult the following link: https://www.fascicolosanitario.gov.it/sites/default/files/docs-pdf/Specifiche-tecniche-per-l-interoperabilit-tra-i-sistemi-regionali-di-FSE-Framework-e-dataset-dei-servizi-base.pdf.

[29] G Pellicanò, 'Sanità digitale, stato dell'arte e prospettive future' (2019) 14, Smart eLab, available at the following link: https://calliope.cnr.it/index.php/smartelab/article/view/79/85.

[30] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico' (2020), 30, federalismi.it, 252.

[31] Before 2016, the year in which the GDPR comes into force, the regulatory references for safety measures were those which can be found in the Personal Data Protection Code, Annex B and the guidelines. In particular, the Guidelines on online reporting (Chapter 6) highlight how: "*The particular sensitivity of personal data processed through online reporting services requires the adoption of specific technical measures to ensure appropriate levels of security pursuant to art. 31 of the Code, without prejudice to the minimum measures that each data controller must in any case adopt pursuant to the Code (art. 33 et seq.) and, in particular, where applicable, those required by rule 24 of the Technical Specifications on minimum security measures, Annex B) to the Code*".

and designed to avoid the risks arising from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, of personal data transmitted, stored or otherwise processed[32].

Therefore, following the lines of the legislator, the system should , in addition to confidentiality, integrity and availability of data, also ensure the security of the same through the adoption of all measures required by the legislation on privacy and by specific measures taken by the Guarantor of the health sector[33].

However, as mentioned above, the data under examination - which, through the FSE, are aggregated virtually and made visible - cannot always count on adequate resources to ensure uniform security measures.

And, therefore, if it is true that, as a result of the above mentioned changes, an attempt is being made to enhance the use of the FSE, it is equally true that it is underestimated that not all the producers called to feed the various FSE use document management and storage systems aligned with the regulations and such as to ensure adequate levels of security and privacy required by the GDPR.

In short, if in theory the FSE tool seems to overcome all the problems existing in the field of electronic medical records (in particular, those concerning the limitations imposed by privacy regulations and the impossibility, even with the patient's consent, to directly transfer the data of the CCE of one hospital to another), in practice, one has to deal with the risks involved, including the risk that during the input phase[34] (for which, please note, the consent of the person concerned is not required), potentially vulnerable data and documents are made available on the FSE, if there is no proper management of the entire life cycle of the document upstream.

In this regard, it can certainly be stated (anticipating what will be said in the last paragraph) that the interoperability of health data - understood as the ability of several systems to exchange information between them and to be able to use them - can be considered the first challenge to ensure that the opportunities of digital health do not remain only as such but are transformed into something concrete.

For the transfer of data suitable for revealing the genetic identity of an individual, the "*Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario*" (Chapter 10) highlight that: "*The particular sensitivity of personal data processed through the FSE/dossier requires the adoption of specific technical measures to ensure appropriate levels of security (art. 31 of the Code)*". The principle of accountability or responsibility, introduced by the European Regulation, requires the preparation of adequate policies on data protection and, therefore, are no longer considered sufficient minimum security measures. In other words, today the Data Controller must adopt technical and organizational measures, including certified ones, that are concrete and always demonstrable, as well as Compliance with these Regulations. By virtue of the principle of privacy by design, it is also necessary that all of the required devices are used from the design phase of the system architecture. In this regard, see the 'Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali' (and in particular the Risk Based Approach and accountability measures (accountability) of Owners and managers).

[32] Opinion on the 'Linee Guida sulla formazione, gestione e conservazione dei documenti informatici' of February 13, 2020 available at the link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283921. The Guarantor clarifies, among other things, that the security measures referred to by the GDPR, in fact, replace the minimum ICT security measures for public administrations set out in the Guidelines issued by AgID in 2017.

[33] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19' (n 28).

[34] The ESF is not fed homogeneously, which is a consequence of different interpretations and implementations by the Regions and Autonomous Provinces, both in reference to the use of document formats and in relation to the set of metadata to be associated with the documents. See in this regard by E Sorrentino and others, 'La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico' (2020) 2(1), Riv. ita di informatica e diritto, 38.

5. The benefits and risks of digital health. In particular, the impact of new technologies on the processing of health data.

Even before the current health emergency, but now all the more so, the pervasiveness of information technologies within the healthcare world has fueled a process of profound renewal based on data.

In addition, the significant expansion of telemedicine solutions and the emergence of innovative solutions have led to informed patient participation and increased their personal well-being.

In fact, thanks to new technologies and the Internet, patients are more informed than ever before about medical conditions and treatments and play an increasingly active role in their care pathways.

One of the main advantages of digital healthcare is the possibility to guarantee complete interconnection, no longer linked to the location of a facility or the times when it is possible to book a medical examination.

This aspect has come to light, as never before, during this pandemic, which has shown how digital technologies - for example, electronic prescription and telemedicine - can allow the continuation of treatment even in a social distancing regime.

From this point of view, the increase of the general interest of health systems to speed up the digitization process is more and more evident; in this way, on the one hand, the reduction of the actual costs of treatment is obtained and, on the other hand, at the same time, a greater accuracy of diagnosis and procedures is guaranteed.

In this process of renewal, modern medical technology has therefore become dependent on the ability to collect and store patient data, image files, videos and a wide range of documents of various types. The inevitable result is the creation of large volumes of data that continue to grow at an increasingly rapid pace, largely unstructured, managed by a variety of different applications and systems and accessible by healthcare facilities, specialists and researchers.

But while it is true that the electronic storage and management of patient data offers substantial clinical and operational benefits, it also introduces new risks.

In particular, although of interest, it should be considered that a technology that is not well governed can cause problems both on an individual and collective level.

On an individual level, if patient data are lost or become inaccessible due to natural disasters or deliberate actions affecting the systems that host them, the consequences can be very serious: think, for example, of the lack of information about a patient's severe allergy to certain drugs.

In addition, knowledge of such "sensitive" data as genetic or health data, can lead to discrimination (think of the employment or insurance relationship) or in any case very relevant prejudices for the person concerned and violate, sometimes irreversibly, that right to the intangibility of one's private life which is the oldest root of privacy.

On a collective level, it must be considered that digitally stored data can also be violated or stolen, exposing patients' medical, personal and financial information and leaving operators vulnerable to ransomware attempts.

Attacks on healthcare information systems - a significant part of *cyber attacks* in our country - can have devastating effects on all citizens, preventing the delivery of healthcare services or, in the case of alteration of patient data, large-scale clinical errors.

Recent research has identified the healthcare sector as one of those exposed to the greatest risks in terms of cybersecurity, because it lacks an organic plan of security and protection, which would be essential in this field, especially in view of the increasing use of cloud computing and artificial intelligence.

In this regard, statistics confirm that the healthcare world is twice as likely, compared to other environments, to suffer from data loss or be the target of *cyber attacks*.

In particular, in the first nine months of 2019, *cyber attacks* on healthcare facilities increased by 60%.

This situation is believed to arise from the high value of patient financial and health data that the health care world processes. More precisely, the value of this type of information is linked to its depth and scope: it includes personal data, date of birth, e-mail addresses, health card numbers, employment data, medical information, insurance data.

As a result, health data has a value in the illegal market that is 10 times higher than credit card numbers and it has been estimated that the average cost of a lost or stolen data record is 136% higher for a healthcare organization than for other types of organizations[35].

As proof of this, precisely in this last period there have been *cyber attacks* linked to the health emergency, aimed at stealing as much health data as possible. And the risks increase, evidently, also due to the greater number of subjects who are called to enter data into the FSE, which, as mentioned, are not only the doctors of the regional health system, but all the health professions that take care of the patient regardless of location. This will inevitably also involve the opening of the FSE to private subjects whose systems will have to interact with the public standard, subject to compliance with the defined safety measures. And it is obvious that the involvement of a wide range of stakeholders in the health sector will also put to the test the current policies for the processing of personal data and the security of the related management systems.

Therefore, if it is true that the FSE is a highly innovative and effective tool, that technological progress makes it possible to put at the service of patients' health, it is also true that its use also entails new pitfalls for patients' right to privacy.

6. The challenges that digital health poses and the perspectives *de iure condendo.*

In light of the risks just highlighted that an "out of control" evolution of digital technology would entail, it is clear that, today more than ever, it is necessary to take note of the need for health data to be guaranteed the correctness of origin and safety of circulation.

It is believed, in fact, that only through strict compliance with the rules on privacy can we attribute the right dimension to information security, to be understood as the set of arrangements to protect all data from accidental events, preventing the vulnerability of the data contained in the various systems to continue to translate into the vulnerability of our physical life[36].

Well then: new needs, new challenges to face.

A first challenge can be considered the need to ensure, as previously mentioned, the interoperability of health data, in order to allow the obtaining of data from multiple sources and to combine them in a usable way. In this sense, a more massive and homogeneous use of the FSE tool would certainly be desirable.

Another objective can be considered the realization of systems in which there is certainty on the authenticity of the information present and available for use by the assigned different operators, so all the necessary precautions must be taken to certify the data entry process.

In addition, it should be sought to exclude the possibility that medical information be accessible and modifiable even by persons who, although part of the medical sector, are not entitled to access such files. With reference to this second challenge, it should be pointed out that the outcome of inspections carried out in recent years in the health sector, has highlighted the presence of abusive access to health records by administrative or medical

[35] *Digital Guardian: The definitive guide to Data Loss Prevention* – Healthcare Edition.

[36] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19', (n 28), 250.

personnel, who had never been involved in the process of patient care and who, for reasons of personal interest, had accessed the same, and then disclosed the information thus acquired to third parties without the knowledge of the person concerned.

Finally, a final challenge can be considered protection from the risk of abusive access by hackers.

In a first step to ensure that these challenges can be accepted (and, above all, won), in a *de iure* perspective, it seems appropriate, first of all, to reflect on the fundamental choices to which our civilizations are called. In this regard, the President of the Guarantor for the Protection of Personal Data has pronounced himself, stating that, on the one hand, the IT risk (which can fatally evolve into clinical risk) must be contrasted with the strictest compliance with the principle of accountability and the criteria of privacy by design and by default, rationalizing the information heritage and the architecture of the processing itself, following the dynamics along the entire chain; on the other hand, the risk of undue access to data in the health record, made possible by an inadequate definition of the perimeter and legitimation profiles of the health professionals themselves, should not be underestimated. In this regard, the Guarantor has recently stated that cases of consultation of health records by unqualified personnel have not been rare, for retaliatory purposes or due to simple, pathological, curiosity[37].

Therefore, the spectrum of data breach should never be underestimated, because data breaches - especially in difficult times such as the current one caused by the Covid-19 emergency - are just around the corner.

One solution, if we want to defend rights and freedoms (of individuals but also of the community), could be to deploy resources on the cybersecurity and national cybernetic security front, because ever increasing information and digital heritage can jeopardize the protection and confidentiality of data processed.

In addition, "cultural" obstacles should also be overcome through the training and updating of health workers so that the health professional does not perceive ICT (Information and Communications Technology) as the fulfilment of or, worse, as a burden on his workload but, and above all, as part of a precise common strategy, the benefits of which affect the whole health system. Healthcare workers must, therefore, understand that among their duties, today, there is not only that of treating people, but also that of taking care of their data. And to this end, health data management strategies are needed to ensure that health data is always protected and available in a reliable, timely and consistent manner.

In the light of what has been said so far, it can undoubtedly be said that the digitization of healthcare is a crucial challenge for our country, with respect to which, however, its fragmentation and inhomogeneity and the absence of an organic security plan have emerged. And this can, without a doubt, represent a major cause of malpractice, making, at the same time, the protection of data and systems a decisive fact of health efficiency.

In fact, taking the FSE as an emblem of this challenge, one cannot fail to emphasize that entrusting the entire medical history of millions of patients to an IT infrastructure is also a not insignificant source of vulnerability, if it lacks adequate protection to prevent undue access, exfiltration or alteration of data: the loss, removal or alteration of health data puts at risk essential databases and, at the same time, violates the most intimate privacy of the individual person, exposing him or her to serious discrimination.

The ultimate goal, therefore, is to make digitization in health care an organic, far-sighted and safe process, thus promoting the efficiency of the system and, with it, the effectiveness of the right to health, overcoming the vulnerabilities of technology and minimizing individual

[37] 'Privacy e dati sanitari. Il Garante: "Incrementare sicurezza, non rari casi di consultazioni indebite Fse' (2020), 26 May, quotidianosanita.it.

and collective risks.