European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 161-170
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 13

*Data Processing in Public Health: The Role of Information Systems**

Luigi Rufo
(Research Fellow at University of Padova)

ABSTRACT This paper addresses the topic of information systems in public health and issues related to the protection of personal data. In particular, a number of information systems found in Italian public health care will be analyzed: for example, the electronic health record, the electronic medical record, and the health file. It will also address the principle of privacy by default and by design and its proper application to properly design a modern information system.

1. *Introduction*

New technologies and the increasing use of digitization in diagnostic and therapeutic pathways are radically changing medical practice.[1] In addition to offering new opportunities for access and continuity of care, these innovations help strengthen prevention, improve quality of life and increase its expectancy. Indeed, current public healthcare is increasingly and boldly trying to rely on new technologies to improve habits, lifestyles, circular methods of communication and information-sharing between doctors and patients.[2]

Smartphones, wearable devices, and social networks have become an appendage of the human body: an "extended body"[3] endowed with evolutionary autonomy and consisting of intangible streams of information that can be processed and exchanged among multiple parties, even geographically distant.

The Covid-19 pandemic has also made evident to the whole world the central role played by digital technologies, which in the field of health protection will have to support the various national governments in meeting the challenge of sustainability and prevention by taking high quality, accurate, informed, and above all quick decisions.

Today, data both in raw and aggregated form represent the "new oil"[4] in public-health policies, as well as the cornerstone of the continuous development towards IoT and artificial-intelligence systems, - tools that may be a central part of any future decision-making, posing the additional challenge of how to improve the ability to "read" and exploit data.

In this framework of continuous development, the digitization and sharing of health data would thus enable a data-driven[5] approach by professionals working in public-health facilities, thus creating not only diagnostic and therapeutic pathways that are more adherent to the needs of patients-especially for those affected by chronic diseases-but also promptly leading to the conclusion of projects related to the study of diseases, as well as research and development of new treatments.

However, in order to outline not only a national and/or regional but also a territorial strategy on improving the use of data, it will be necessary to focus attention toward several unavoidable points of observation, leveraging on both currently available information-technology standards and collaboration among the various public-health players.

Indeed, first of all it will be necessary to

* Article submitted to double blind peer review.

[1] T. Schael, *Sanità elettronica e servizi digitali al cittadino. La rivoluzione delle ricette e dei certificati di malattia*, in *eHealthcare*, n. 3, 2009, 13.

[2] See A.D. Weston and L. Hood, *Systems biology, proteomics, and the future of health care: toward predictive, preventative, and personalized medicine*, in *Journal of Proteome Research*, n. 3, 2004, 179-196; P. Cappelletti, *La Medicina Personalizzata fra ricerca e pratica clinica: il ruolo della Medicina di Laboratorio*, RIMeL/IJLaM, 2009, n. 5 (Suppl.), 26-32; Q. Tian and Others, *Systems cancer medicine: towards realization of predictive, preventive, personalized and participatory (P4) medicine*, in *Journal of Internal Medicine*, n. 271, 2012, 111-121.

[3] M. Mancarella, *eHealth e diritti. L'apporto dell'Informatica giuridica*, Rome, Carocci, 2014, 15.

[4] A. Charles, *Tech giants may be huge, but nothing matches big data*, in *The Guardian*, 2013.

[5] See Z. Hou and Z. Wang, *From model-based control to data-driven control: Survey, classification and perspective,* in *Information Sciences*, 2013, 3-35; S.L. Brunton and J.N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*, Cambridge, Cambridge University Press, 2017, 414- 416; V. Breschi, A. Chiuso and S. Formentin, *The role of regularization in data-driven predictive control*, in *arXiv preprint*, Singapore, 2022.

take into consideration the technologies and procedures already implemented by hospitals and local health trusts in order to avoid the use of obsolete models or tools. Then it will be necessary to consider, step by step, the current technological framework with the aim of reaching possible and complete interoperability of information systems and public databases.

Undoubtedly, in Italy several tools, each according to its level of use, play a key role in the management of data related to citizens' health: Electronic Health Record (so-called Fascicolo Sanitario Elettronico - FSE), which is of regional level, Health File (so-called Dossier sanitario elettronico - DSE), and Electronic Medical Records (so-called Cartella clinica elettronica - CCE) specifically linked to health facilities.

Such information systems, through their application potentials in part still unexplored, are key strength in the public-health sector being based on the centrality of patients and sharing and management of their clinical information. They allow to promote self-determination (so-called "patient empowerment"[6]), which implies a process of personal development in which patients, in a partnership relationship with health professionals, are provided with knowledge, skills, and greater awareness of health treatments. In other words, an information flow that is not uni-directional but bi-directional or, even more precisely, circular can be developed.[7]

With regard to this issue, Italian law makers - in four first historical stages - i) Decree Law No. 158 of September 13, 2012; ii) Decree Law No. 179 of October 18, 2012 which provided, in Section IV, Art. 12 the FSE and Surveillance Systems in the Health Sector - and Art. 13 - Medical Prescription and Medical Records; iii) Decree "Fare" approved in June 2013; iv) Presidential Decree of September 29, 2015 no. 17, which defined the rules by which the Regions must set up their own FSE systems - was designed to adopt measures aimed at concretely introducing into the national law tools that, besides improving efficiency, effectiveness and appropriateness of care, help patients keep their data and information up-to-date in their own health records, managed in total autonomy and self-determination.[8]

In this frame of reference, it is also interesting to take into account the provision of the Italian Data Protection Authority ("Privacy Authority") which, when called upon to express an opinion on the DSE, defined it as one of the "numerous initiatives under way to improve the efficiency of the health service by a further development of networks and more extensive IT and telematic management of acts, documents and procedures".[9]

We can thus argue that clear, reliable and up-to-date data and information are a strategic asset to enable public healthcare providers to optimize their care processes and provide their patients with increasingly better services while also avoiding errors.

2. *Information systems in public health: from the electronic medical records to electronic health record*

An information system can be technically defined as a set of interconnected elements that collect (or search), process, store and distribute information to support decision-making and control activities in healthcare organizations.[10]

Before the introduction of electronic tools,

[6] R.M. Anderson and M.M. Funnell, *Patient empowerment: reflections on the challenge of fostering the adoption of a new paradigm*, Patient Education and Counseling, 2005, 153-157; L. Buccoliero, *E-HEALTH 2.0 - Tecnologie per il patient empowerment*, in *Mondo digitale*, 2010; G. Ferrando, *Diritto alla salute e autodeterminazione, tra diritto europeo e costituzione, in Politica del diritto*, XLIII, 1, 2012; L. Rufo, *Profili giuridici del Personal Health Record: tra diritto all'autodeterminazione e tutela della privacy*, in C. Faralli, R. Brighi and M. Martoni (eds.), *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Turin, Giappichelli, 2015, 321-333.

[7] L. Rufo, *Il Dossier sanitario elettronico. Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, Bologna, Il Mulino, 2018, 4.

[8] See M.G. Virone, *Il Fascicolo Sanitario Elettronico. Sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Rome, Aracne, 2015, 145.

[9] Garante Privacy, *Registro dei provvedimenti n. 331 - 4 June 2015*, [doc. web n. 4084632].

[10] K. Laudon, *Management dei sistemi informativi*, Milan, Pearson, 2006, p. 17-19; N. Agabiti, M. Davoli, D. Fusco, M. Stafoggia and C. A. Perucci, *Valutazione di esito degli interventi sanitari*, in *Epidemiologia & Prevenzione*, Milan, Inferenze, 2011, n. 35, 1-80; C. Caccia, *Management dei sistemi informativi in sanità*, Milan, McGraw-Hill, 2008; C. Caccia and G. Nasi, *Il sistema informativo automatizzato nelle aziende sanitarie*, Milan, McGraw-Hill, 2002; L. Buccoliero, C. Caccia and G. Nasi, *e-He@lt: percorsi di implementazione dei sistemi informativi in sanità*, Milan, McGraw-Hill, 2005; A. Teti and G. Festa, *Sistemi informativi per la sanità*, Milan, Apogeo, 2009.

information management took place on paper, thus requiring the work of recording, storing documents and searching for them, with consequent limitations from the point of view of efficiency. The advent of information and communication technologies (ICT) has significantly improved the situation. Data can already be *ab origine* provided with the meaningful "form", which being useful to get information, results in improved health-care services to protect both individual and community health.

The essential elements shaping an information system are: data (essential component of the system and initially not yet processed); information (set of processed data); people (the recipients of the processed information); tools (the set of equipment capable of transferring information from one subject to another); and the processes (set of criteria that allow to understand the way in which data is collected and processed).

However, depending on the state of computerization of care processes, various strategies and models for organizing clinical data can be envisaged.

Among the systems of electronic recording/archiving of patient clinical data used in public-health care, the following are in place: the Electronic Medical Record (so-called CCE); Health File (so-called DSE) and the Electronic Health Record (so-called FSE).

The model best known so far in the national and international context is precisely the so-called Electronic Health Record, which is characterized by its organizational structure built on a unified corporate clinical "data repository". In such a repository, all health information produced in the various therapeutic processes, which see the patient as a primary actor, is brought together and is accessed by the several health professionals working in the facility.

Thus, there has been a shift in recent decades from the design of healthcare institution "episode records" (Electronic Medical Record) to the creation of healthcare institution "system records" (Electronic Health Record), which can offer a longitudinal view of patient health. This model collects and stores clinical data and information of patient pathways in a Data Base (DB).[11]

2.1. *Electronic medical records*

The medical record constitutes the official and legally-recognized document for the systematic and functional collection of data on a patient's medical history within a public hospital. In the European sphere, the European Commission's Recommendation of July 2, 2008 on cross-border interoperability of electronic medical records systems, under Article 3(c), defines CCE as: "a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes".[12]

At the national level, though there is no precise definition, doctrine and jurisprudence agree that the CCE is "a public document having the function of a diary of medical intervention and the relevant clinical facts so that the facts must be recorded in accordance with their occurrence".[13]

The above is also reflected in Article 26 of the new Code of Medical Ethics, which provides that "The medical record of public and private health providers must be drawn up clearly, with punctuality and diligence, in compliance with the rules of good clinical practice and contain, in addition to any objective data related to the pathological condition and its course, the diagnostic-therapeutic activities provided. The medical record must record the manner and timing of information as well as the terms of consent of

[11] Collection of data managed through a Data Base Management System (DBMS). The data are structured and linked together, at the logical level, in accordance with the representation model (e.g. relational) adopted by the DBMS and, at the physical level, reside on memory devices organized in particular structures. Users interface with the database through a Query Language (e.g. SQL). For more information: P. Atzeni, S. Ceri, S. Paraboschi and R. Torlone, *Basi di Dati: modelli e linguaggi di interrogazione,* McGraw-Hill, Milan, 2013; R. Ramakrishnan, *Database Management Systems*, McGraw-Hill / Asia, 2004; R.A. Elmasri and S.B. Navathe. *Sistemi di basi di dati Fondamenti,* Addison Wesley, 2004.

[12] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (2008/594/CE).

[13] B. Primicerio, *La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità*, in *Il Diritto sanitario moderno*, 2004, 207; V. Vaccaro, *La cartella clinica*, in *Trib. amm. reg*., 2003, 180; G. Rocchietti, *La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy*, in *Minerva medicolegale*, 2001, issue 1, 15; O. Bucci, *La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici*, Santarcangelo di Romagna, Maggioli, 1999.

the patient - or his or her guardian - to diagnostic and therapeutic proposals; it must also record the patient's consent to the processing of sensitive data, with particular regard to cases of enrollment in an experimental protocol".

In light of this, computerization of the medical record, with a view to making health-care processes more efficient, flexible and responsive to people's needs, is part of a broad context of internal reorganization in hospital facilities, also enabling the introduction of important improvements in data management, complying with the requirements of completeness and integrity.

However, over time, the CCE has been seen as a mere evolution of the Paper Medical Record (so-called Cartella clinica cartacea - CCC); but it should be noted, instead, that it represents one of the most accurate tools of eHealth for systemic and structured management of data referring to the clinical history of patients in in-patient or out-patient settings by promoting the continuity of patient care in the same health facility through the sharing and retrieval of clinical data recorded.

The added value of the CCE with respect to the CCC is well outlined in a textual passage of the Guidelines of the Lombardy Region, in the following terms: "The CCE is therefore configured as an integrated corporate IT system, to be understood as a transversal tool for the various care processes, replacing the paper medical record, which on the one hand meets the requirements and functions of the latter, and on the other hand solves some critical issues related to it, offering opportunities to increase the value through integration with other IT tools. It is important to recognize the electronic tool as having its own dignity, which also determines a strong difference in the way it fulfills its functions compared to the paper tool. The electronic tool today is capable of fulfilling all the tasks formally defined for the paper medical record, but it is necessary and desirable that it does so differently, that is, according to the logic of effective and efficient electronic data management. For this reason, the concept of the electronic medical record tool as the mere "digitizer" of paper, to be implemented without an adequate review of internal processes, is reductive-if not erroneous-and does not allow the potential in terms of integrated information management, timeliness, automation, and simplification offered by the ergonomics of the digital tool to be exploited".[14]

Typically, a CCE consists of several functional blocks such as administrative documentation; informed consent; initial medical and nursing clinical framing; clinical management (vital-parameter documentation, invasive-procedure documentation, nursing-care sheets, medical reports, etc.); medication-therapy management (often delegated to an external, enterprise-integrated application); and transfer and discharge documentation.

Another relevant element, referred to in the privacy regulations, is that appropriate safeguards must be established with respect to access to data by health professionals, patients and third parties, with regard to measures of a technical nature such as identification, authentication and authorization of the individuals who will have access to the system. An additional aspect, which is very important for privacy, is the need to separate the different categories of data that may be included in the electronic medical record, providing a modular structure to be aligned with the various purposes of processing and/or the individuals who may access the data.

Lastly, an important aspect that should not be overlooked concerns the rules on the processing of personal data which give primary importance to the principle of self-determination on the use of the Electronic Health Record, which leads to the obligation to plan appropriate moments for informing patients to express true consent (opt-in) or forms of dissent (opt-out).

It should be noted that the Italian Data Protection Authority, called upon to express an opinion on the mechanisms that a CCE system must implement, has stated that "in addition to compliance with privacy regulations, IT security requirements must also to be met, which may vary in relation to the use that is made of the data and with respect to possible data transfers to third countries".[15]

2.2. *Health file*

As early as 2009, although in the - still persisting - absence of a legal definition at the national level, the Privacy Authority felt the

[14] Regione Lombardia, *Linee guida per la Cartella Clinica Elettronica Aziendale*, v. 02.1, 2012.
[15] Garante Privacy, *Registro dei provvedimenti n. 131 - 15 February 2007,* [doc. web n. 1607201].

need to determine specific guarantees, responsibilities and rights with reference to the Electronic Health Record. Against this background, the Authority adopted the Guidelines on Electronic Health Record and Health File.

Specifically, these Guidelines defined the electronic health record as "the tool established at a health-care organization as a single data controller (e.g., hospital, health trust, nursing home) within which several professionals operate, through which information is made accessible, inherent to the health status of an individual, relating to present and past clinical events (e.g., laboratory reports, documentation relating to hospitalizations, emergency department access), aimed at documenting the clinical history".[16] In other words, the health file was intended as a collection of present and past clinical events related to an individual patient and processed exclusively at a single health facility, with a view to documenting patients' entire clinical history.

However, the significant increase in the use of this information system for the management of health records in public facilities on the one hand and, on the other, the results of inspections which caused many sanctions led the Privacy Authority in 2015 to provide new and specific Guidelines on the Health File.[17]

By this way, also thanks to the Privacy Authority, as of today DSE can be appropriately framed as a digital tool related to eHealth whereby it is possible not only to store the patient's entire medical history with reference to the services provided within a given health facility, but also to keep track of the diagnostic, therapeutic and care pathway throughout patients' lifetime.[18]

The usefulness of DSE is undeniable: just think of the examination results-sometimes invasive and not repeatable in the short term-already carried out on the person concerned and to which the doctor will be able to have access, without necessarily having to repeat the same, with enormous savings of both time and money; or, again, think of the advantage deriving from the implementation of this tool with reference to subjects suffering from chronic pathologies, of which the doctor will thus be able to become immediately aware by adopting all due precautions aimed at reducing and/or eliminating the risk of error in the administration of specific health treatments.

However, as also pointed out by the Privacy Authority, in order for the health files to be effective in the diagnosis and treatment of patients, it is necessary that they be created in such a way as to ensure the certainty of the origin and correctness of the data, as well as the accessibility of the same only by legally-entitled persons. As a consequence, the Privacy Authority considered the creation of this tool optional, which implies that, in the absence of an explicit self-determination of the interested party to the creation of the same, it would be impossible to open a file as DSE. In any case, failure to consent to the establishment of DSE cannot in any way affect access to medical care, which is a right enshrined in the Italian Constitution. On the contrary, in case of consent to the creation of DSE and entering data, the purposes to be pursued must be exclusively linked, as a guarantee for patients, to the prevention, diagnosis, treatment and rehabilitation of the person concerned, without further possible uses.

However, the Privacy Authority has actually decided it is possible to pursue administrative purposes (e.g., booking through the CUP or payment for a health service) through DSE, but it must be structured in such a way that the administrative data is separated from the health data and that different enabling profiles are provided for the individuals who have access to the DSE, due to the function of the operations they can perform.

A further major element is the need to make sure that the person concerned be able to decide to obscure certain health data or documents, which will therefore not be visible and consultable through Dossier sanitario elettronico by health professionals who access it; or else, detailed access "enabled" from time to time by the patient should be provided for.

2.3. *Electronic health record*

The Electronic Health Record, provided for in Article 12, Decree Law No. 179 of October 18, 2012 concerning "Further Urgent

[16] Garante Privacy, *Linee guida in tema di Fascicolo sanitario elettronico e dossier sanitario,* [doc. web n. 1598313].
[17] G.U. n. 164 of 17 July 2015, more information: www.gpdp.it, [doc. web 4084632].
[18] L. Rufo, *Il Dossier sanitario elettronico. Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, 25.

Measures for the Country's Growth," is a tool whereby citizens can track and consult their entire-life health history, sharing it with health professionals to guarantee a more effective and efficient service.

All the information and documents that make up FSE are made interoperable to allow it to be consulted and populated throughout the country, not just in the patient's region of residence. This offers patients greater freedom in choosing care and sharing information, all of which is available through access to FSE by health-care professionals.[19]

In addition, access to FSE by health professionals, especially in emergency situations, allows them to know everything they need to intervene promptly and guarantee the health outcome. In other words, in the FSE system, the patient is at the center of the system with his/her health history and every medical action concerning him or her tracked and codified, also avoiding the repetition of unnecessary clinical investigations. All this is done in compliance with the conditions defined by the persons themselves at the time of the first access to FSE and such conditions can be changed at any time. Patients, in fact, can choose who is authorized to consult their FSE, under what conditions and also what data, choosing, therefore, also to obscure some information. In addition, they can view who accessed FSE and when.

FSE is therefore defined in the national legislation as the set of health and social-health data and digital documents generated by present and past clinical events concerning the patient, and has as its main objectives: to facilitate patient care; to offer a service that can facilitate the integration of different professional skills; and to provide a robust information base.[20]

The FSE also pertains to a wide range of activities, regulated by the Ministry of Health, related to the delivery of health services. Specifically, it is aimed at the overall improvement of the quality of services concerning: prevention, diagnosis, treatment and rehabilitation; study and scientific research in the medical, biomedical and epidemiological fields; health care planning, checking of the quality of care and evaluation of public-health care.

In this regard, it is interesting to make some comments on the implementation and utilization of indicators of FSE, which has had a strong implementation momentum with the Covid-19 pandemic.

Specifically, the implementation indicators aim to represent the state of progress about the implementation of the regional FSE, whereas the utilization indicators are aimed at monitoring the actual level of use and diffusion of the FSE throughout the country by citizens, physicians and health-care providers. On the implementation side, we must note that, out of twenty regions, as many as fifteen regions have reached 100% of the implementation outcome, four of them have reached 90%, and fortunately only two regions scored 80%.

On the other hand, looking at the indicators of utilization, there are significant differences among the several actors analysed. In particular, a general backwardness emerges in the use of FSE by physicians and by citizens. Better data is found for use by Health Authorities, although in several regions data is close to zero.[21]

It is undeniable that from the current scenario of FSE implementation, a partial use of the same emerges compared to its use as a support for patient care. In fact, FSE should be viewed as a true decision-making tool capable of collecting and making available the entire medical history of a patient.

This is especially true in the long run since, at the research level, FSE could lead toward the creation of a national health repository that may ensure the use of data for health research and be a key source of information.

On the side of data-protection regulation, it should be noted that during the pandemic period an important innovation was introduced. Indeed, in order to accelerate the activation and use of the FSE by all patients, Article 11 of Decree Law No. 34 provided that, as of the date of publication of the decree, the activation and population of the FSE will take place automatically, with the elimination of the "consent to entering" so that

[19] P. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trent, University of Trent, 2011; L. Califano, *Fascicolo sanitario elettronico (Fse) e dossier sanitario: il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in *Sanità pubblica e privata*, Santarcangelo di Romagna, Maggioli, issue 3, 7-22, 2015.

[20] M. Moruzzi, *Il Fascicolo Sanitario Elettronico in Italia. La sanità ad alta comunicazione*, Milan, Il Sole 24 Ore, 2011.

[21] More information: www.fascicolosanitario.gov.it/

patients can easily consult their social-health documents, even if generated by public-health facilities located outside the region they come from, thanks to the interoperability ensured by the Health Insurance Card System. In addition to this, regardless of the consent of the patient, health-governing bodies can access pseudonymized data in FSE to carry out related institutional functions (e.g., care planning, health-emergency management).

Furthermore, on October 5, 2020, following this important regulatory change, the Privacy Authority issued a specific opinion regarding the process of populating FSE, with respect to the issue concerning the entering of data prior to May 2020, stating that, in order to guarantee the rights of data subjects, an adequate information campaign had to be carried out at the national and regional level aimed at: i) making data subjects aware of the characteristics of the processing carried out through FSE, with particular reference to the new features introduced by the applicable regulations; ii) ensuring that the data subject could exercise the right to object to populate FSE with health data generated by clinical events prior to May 19, 2020, within a predetermined period, not less than 30 days.

3. *Privacy in public health information systems*

The possibility, inherent in ICT technologies, to process significant amounts of data at high speed and often without capillary control, even going so far as to trace detailed profiles of data subjects, has produced a consequent acceleration also in regulating the right to protection of the personal sphere of individuals.

Hence, it seems appropriate to analyze the context and development of information systems and their application in the public-health sphere by considering the European Data Protection Regulation No. 679 of 2016, which constitutes the new primary source of reference for the protection of personal data of individuals.

This new law has introduced clearer rules and stricter criteria with the aim of ensuring greater assurance to the data subject with respect to data processing through new information society technologies and better regulatory harmonization and alignment in the European context.

Indeed, while on the one hand the development of computer systems for storing and organizing data has positively favored access to care and improvement in treatment pathways, on the other hand, however, it has generated new dangers in terms of reliability and security, leading to the introduction of more stringent custody obligations on the part of operators, also imposed by the existing data protection legislation.[22]

Thanks in part to the GDPR regulations, key principles for the proper processing of personal and health data through information systems have taken shape, and they are essentially: a) minimization of the collection, use, disclosure and storage of users' identifying data;[23] b) participation and active involvement of users, among other things, allowing the exercise of powers of control during the lifecycle of processed personal data; and c) enhanced security of information. These principles should then be summarized under the broader definition of privacy by design and privacy by default, which, after a laborious legislative process that began on January 25, 2012, resulted in Article 25 of the GDPR, headed "Data protection by design and protection by default".[24] Yet, it should be noted how this Article, while providing a cogent and innovative contribution compared to the past, largely recalls the intrinsic essence of the principle of necessity in data processing, already contained in Article 3 of the Italian Privacy Code and extensively described in the provisions of the Privacy Authority, which states: "*information systems and computer programs shall be configured reducing to a minimum the use of personal data and identification data, so as to exclude their processing when the purposes pursued in individual cases can be achieved by means of, respectively, anonymous data or appropriate modalities that allow the data subject to be identified only in case of necessity*".[25]

[22] A. Cavoukian, *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, Information and Privacy Commissioner of Ontario, 2009.

[23] R. D'Orazio, *Protezione dei dati by default e by design*, in Sica and D'Antonio e Riccio (eds.), *La nuova disciplina europea sulla privacy*, Milan, Giuffré, 2016, 79.

[24] More information: EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, ver. 2.0., 20 October 2020

[25] In order to clarify these concepts expressed in Article 25, it's necessary to read Recital 78 of the GDPR: "The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures

This is a precept that, anticipating by a few years the formalization of the broader concept of privacy by design and by default, entails an important consequence in the context of data processing carried out with automated systems. Indeed, according to the principle of necessity, information systems and computer programs must be configured to handle data anonymously-for example, through the use of an alphanumeric code-so that the data subject cannot be directly identified.[26]

However, particularly interesting for the purposes of the present analysis is to note how this concept is also in wide use in the field of digital health, with the peculiarity that its fulfillment in this sector is not relegated to the technological aspect of information-systems design and development alone, but also affects the phase of implementation and adaptation of the facilities' premises. Take, for example, server rooms or offices where there is a risk, through unauthorized access, of illicit disclosure of the sensitive data of the persons concerned.

What distinguishes the concept of privacy by design and privacy by default[27] are undoubtedly seven pivotal "elements": Proactive not reactive; Privacy as the default setting; Privacy embedded into design; Full functionality - positive-sum, not zero-sum; End-to-end security - full lifecycle protection; Visibility and transparency - keep it open; Respect for user privacy - keep it user-centric.[28]

3.1. *Proactive not reactive*

The first element of privacy by design is characterized by actions with a proactive rather than reactive approach. Indeed, it is much more useful to prevent and address critical issues before they turn into actual, active harm, so that promptness in acting, even before the problem may arise, is an added value in design and characterizes this principle by favoring the protection of information.

However, it is relevant to emphasize that the above is valid only if there is constant monitoring of the development project and willingness to set high standards of data protection and security.

In the public health sector, it is easy to believe that this principle is crucial: the prevention and anticipation of possible breaches of health data through abusive access to information systems makes it possible to achieve a perception of high reliability of healthcare facilities among patients, as well as to reduce/eliminate subsequent architectural interventions, thus saving additional costs for possible recovery.

3.2. *Privacy as the default setting*

Privacy by design through the default setting of an IT system seeks to achieve the highest level of personal-data protection. Based on this principle, the user will be able to rely on the setting built into the system to maintain his or her degree of privacy without having to take any action.

For users this is an important principle as they are the primary actors in the management of their own information.

The concepts on which privacy by default is based are privacy protective and data minimization.[29] The first concept concerns the

be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders".

[26] F. Bravo, *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia, C. Irti and A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Singapore, Springer, 2022, 85-95.

[27] F. Bravo, *L'architettura del trattamento e la sicurezza dei dati e dei sistemi*, in Cuffaro and D'Orazio and Ricciuto (eds.) *I dati personali nel diritto europeo*, Turin, Giappichelli, 2019, 823.

[28] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, Information and Privacy Commissioner of Ontario, 2010, 12.

[29] Principle derived from Article 6 paragraph 1 (b) and (c) of Directive 95/46/EC and Article 4 paragraph 1 (b) and (c) of EC Regulation No. 45 of 2001 and provides that personal data must be *"collected for specified, explicit and legitimate purposes*" and must be "*adequate,*

view that the design of an IT system takes into account a specific and effective purpose that legitimizes the collection of data. The second, on the other hand, mandates that data be processed only where strictly necessary. This encourages the implementation of a true prevention mechanism, which in the health care field could be implemented, for example, by using pseudonyms to identify and/or de-identify patients or provide for the automatic hiding of reports uploaded to healthcare organizations' information systems.

3.3. *Privacy embedded into design*

This principle states the importance of considering data protection and its management as an essential component in the design of a system, but without diminishing the functionality of the system.[30]

In order to fully stick to this principle, it is necessary to pursue the continuous updating of good implementation practices, standards and regulatory acts, such as laws and regulations, also taking into account technological progress.

In healthcare, this is achievable through the updating of standards and Guidelines for supporting the development and implementation of IT systems.

3.4. *Full functionality-positive-sum, not zero-sum*

Privacy by design via the development of this principle points to a vision that aims to reconcile all the interests and objectives involved in the development of an IT system. In other words, what it aims to achieve is the demonstration that privacy and security can coexist without having to forcibly choose to protect one aspect whilst neglecting another. A turning point is the creation of non-invasive systems that maintain only the strictly-necessary information.

3.5. *End-to-end security - full lifecycle protection*

Security is a key concept, and without it no responsibility and no rights could be assigned. In fact, only with the application of security-related elements privacy by design can ensure the full lifecycle of information to the end.

In light of what has just been said, the most delicate role is played by developers and designers, whose task is to apply security methodologies in order to eliminate, or at least reduce, not only the risk of theft but also the complete or partial deletion of data.

3.6. *Visibility and transparency*

Privacy by design seeks to ensure transparency to all stakeholders. The principle of transparency requires that information intended for the public or data subject be concise, easily accessible and easy to understand, and that plain and clear language be used. This principle is a relevant feature and leads to the concept of accountability. In other words, the data controller is required to demonstrate that the processing, through privacy policies, has been carried out in accordance with data-protection regulations.[31]

3.7. *Respect for user privacy - keep it user-centric*

As a first step, privacy by design requires designers and developers to give priority to users' requests and interests.[32] This way, the concept of "user-centricity" takes on two different meanings: the first, as the user's right to exercise control over his/her own information; the second, in terms of a factor that forges a system around the figure of the user, and thus around his/her needs. It follows that if users are recognized to have a way to manage information about themselves quickly and easily, the system will have to enable this outcome.

In healthcare, it is now a well-established fact that, via consent to medical treatments, the patient can almost totally self-determine his/her choices and be the focus of healthcare services; in the area of consent to data processing, the same approach should operate.

relevant and not excessive in relation to the purposes for which they are collected and/or subsequently processed."

[30] U. Pagallo, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Cham, Springer, 2012.

[31] G. Finocchiaro, *L'accountability nel regolamento europeo,* in Barba e Pagliantini (eds.), *Delle persone. Commentario del Codice civile*, Vol. II, Milan, Giuffrè, 2019.

[32] R. Brighi e M.G. Virone, *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica,* in *A Matter of Design: Making Society trough Science and Technology*, Milan, Open Access Digital Publication by STS Italia Publishing, 2014.

4. *Conclusions and future perspectives*

IT, process innovation, person-centeredness and privacy are undoubtedly the four main drivers that are directing and changing "2.0" healthcare services within public health organizations, with tangible outcomes of improved patient management and clinical-risk prevention.

In addition, it should be added that the European Commission in February 2020 drafted a European data strategy, which is considered a central element of the technological transformation so much desired in the European NextGenerationEU program.[33]

That strategy has included healthcare among other areas, which was deemed "essential for making progress in the prevention, detection and treatment of diseases, as well as for making informed and evidence-based decisions to improve the accessibility, effectiveness and sustainability of health care systems"[34].

But there is more. Indeed, a corollary to the goal of this strong proactive boost of the European Commission is to ensure a reduction in health costs through better access, use and reuse of health data, with the long-term vision of redistributing resources by reprogramming ah essential levels of care.[35]

In this framework, the information systems of public healthcare organizations will play a key role since all clinical data produced by electronic health-record systems, medical devices and artificial-intelligence systems will be able to lead to their reuse also and especially for research and innovation (so-called secondary use of data).[36]

As also stated by the president of the Privacy Authority Prof. Pasquale Stanzione, "the digitization of healthcare is, in this sense, an extraordinary opportunity for development, innovation, competitiveness, to be promoted for the efficiency and universality of care and for better planning of healthcare expenditure. However, digital health must be realized within an organic and far-sighted project of health governance, which minimizes cyber risks and promotes selective data sharing, for the purpose of promoting research, but with due caution to avoid any possible re-identification of data subjects".[37]

In this framework with still uncertain contours, abidance by privacy legislation and its guiding principles may well represent the crux around which "expert" information systems can be developed. Sharing data in a European health-data space will make it possible to give more value to health not only as a fundamental right of individuals but also in the interest of the community in order to find immediate answers to common situations in the context of public health, as happened in relation to the Covid-19 pandemic but obviously always by fulfilling the centrality of human persons and their dignity.

[33] Regulation (EU) 2021/241 of the European Parliament and the Council 12 February 2021 establishing the Recovery and Resilience Facility.

[34] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM(2022) 197/2 final.

[35] V. Di Felice, *Lo spazio europeo dei dati sanitari*, in *Nota su atti dell'Unione europea*, Servizi studi del Senato, n. 102, July 2022.

[36] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020.

[37] More information: Garante Privacy, *Sicurezza del dato sanitario e condivisione* [doc. web n. 9747071].