Chapter 3 Data protection and the e-health sector

3.1 Introductory remarks

This chapter is dedicated to the healthcare domain. Health is a critical part of people's well-being[716]. According to the WHO, health is a "state of complete physical, mental and social well-being and not merely the absence of disease or infirmity"[717]. Article 35 of the EU Charter of Fundamental Rights states that "everyone has the right of access to preventive health care and the right to benefit from medical treatment" and that "a high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities"[718]. The right to access to healthcare is at the core of human well-being.

According to Abedjan *et al.*, public expenditure on healthcare will increase by one third by 2060 worldwide due to a rapidly ageing population[719]. In recent years, healthcare provision has been improved by the use of digital technologies[720]. Healthcare is one of the more data-intensive

716 *See* further on OECD, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*.

717 *See* the comment on the definition in Daniel Callahan. "The WHO definition of 'health'". In: *Hastings Center Studies* (1973), pp. 77–87.

718 This last sentence is also used in Article 168 of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union.

719 *See* Abedjan et al., "Data science in healthcare: Benefits, challenges and opportunities", p. 6. Other statistics are reported by Y. Quintana and C. Safran. "Global health informatics — an overview". In: *Global Health Informatics*. Elsevier, 2017, pp. 1–13. ISBN: 9780128045916.

720 *See* the evolution of the digitalisation of healthcare in D. Sigulem, M.P. Ramos, and R. de Holanda Albuquerque. "The New Medicine: From the Paper Medical Record to the Digitized Human Being". In: *Global Health Informatics*. Elsevier, 2017, pp. 152–167. ISBN: 9780128045916.

721 The World Health Organisation provides a portal on the Global Health Observatory with data and detailed indicators. *See* <www.who.int/data/gho>. Last accessed 06/10/2021.

sectors[721]. Even though ICTs have a great potential for supporting healthcare[722], some privacy and security concerns arise[723].

The first part of this chapter addresses some issues that have emerged from the use of technology for health purposes. Generally, the risk level for the processing of personal health data is high. Because of the sensitive nature of personal health data, special attention should be paid to privacy and data protection concerns of health and health-related data. Then, the Chapter focuses on the data protection law for the processing of personal health data in the EU legal framework. After these theoretical considerations, the Chapter presents the case study of the book, a specific e-health technology called Electronic Health Record system. The state of the art, the applicable rules, and cross-border use of this technology are examinated. Finally, the Chapter briefly concludes with other consideration on balancing the right to data protection against public interests in the healthcare context.

3.2 Data protection concerns of e-health technologies

Since the 1990s, ICTs have played an important role in improving access to and quality of healthcare, and the neologism *e-health* connects the use of digital technologies to this sector[724]. As mentioned in the first pages

722 *See* for some statistics OECD, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*.

723 *See ex multis* EXPH Expert Panel on effective ways of investing in Health. *Assessing the impact of digital transformation of health services*. Luxembourg: Publications Office of the European Union. 2019; OECD, *OECD Recommendation on Health Data Governance*; Council of the European Union, EU Council, *Council conclusions on Health in the Digital Society — making progress in data-driven innovation in the field of health*; Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection"; Arak and Wójcik, *Transforming eHealth into a political and economic advantage*; Adams, Purtova, and Leenes, *Under observation: The interplay between eHealth and surveillance*; Paolo Guarda. "Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context". In: *Trento Law and Technology Research Group Research Paper n. 23* (2015); Lowrance, *Privacy, confidentiality, and health research*.

724 Aceto, Persico, and Pescapé, "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges", pp. 125, 128.

of this work, the digital processing of health data creates both enormous opportunities and critical challenges.

The digitisation should be considered as more than a technical process since it involves both ICTs and practices, services and healthcare-related processes[725]. For this reason, the definition of e-health provided by the European Commission is[726]:

> "The use of ICT in health products, services and processes combined with organisational change in healthcare systems and new skills, in order to improve health of citizens, efficiency and productivity in healthcare delivery, and the economic and social value of health".

In theory, the opportunities of the digital processing could be summarised as better clinical outcomes, more tailored therapeutic responses and more effective disease management[727]. E-health strengthens the quality and the effectiveness of the healthcare provision by improving service quality and health benefits, and by saving time[728]. Health Information Technologies (HITs) can respond to the needs of patients most effectively and efficiently[729]. E-health systems can also reduce costs and improve productivity of the health sector by reducing medical errors, improving billing and record-keeping, and decreasing unnecessary care[730]. It has been noted

725 For a description of the "digital transformation" of healthcare *see* Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*, pp. 13–14.

726 European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century", p. 3.

727 This summary is provided by Abedjan et al., "Data science in healthcare: Benefits, challenges and opportunities", p. 16. According to a study by Polityka Insight, the advantages are: "improved quality of care; better planning and resource allocation; cost efficiency; more efficient health landscape; enhancing the evidence base for health service delivery and policy making; real-time monitoring; providing better, tailored and personalized services; and preemptive measures". *See* Arak and Wójcik, *Transforming eHealth into a political and economic advantage*, p. 6.

728 Guarda, "Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context", pp. 1, 7. *See* also Paolo Guarda. "I dati sanitari". In: *I dati personali nel diritto europeo*. G. Giappichelli Editore, Torino, 2019, pp. 591–626. ISBN: 9788892112742, pp. 614–615.

729 Concetta Tania Di Iorio and Fabrizio Carinci. "Privacy and health care information systems: where is the balance?" In: *eHealth: Legal, Ethical and Governance Challenges*. Springer, 2013, pp. 77–105. ISBN: 9783642224744, p. 77.

730 *See* EC European Commission. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and*

that "anytime" and "anywhere" monitoring, diagnosis and treatment are part of an "on-demand" culture which characterises the world of online commerce[731]. The traditional workplace has been completely redefined, the demand for health and social services increases, and new mobility phenomena, such as "hospital shopping", appear[732]. At the EU level, digital technologies have deeply changed the provision of healthcare by facilitating the sharing of data in more effective ways across countries and enabling new medical treatments[733]. E-health is a key e-strategy of the EU[734]. It represents a new industry of the digital age with great market potential.

---

the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area. European Commission. Brussels: COM (2004), 356 final. 2004, p. 6. The Commission made reference to the detailed study by Patricia Danzon and Michael Furukawa. "e-Health: effects of the Internet on competition and productivity in health care". In: *The economic payoff from the internet revolution*. Brookings Institution Press, 2001, pp. 209–244. ISBN: 9780815700654. This study has proven the major impact of the Internet on the health care sector by analysing the economic trends of the market.

731 *See* Ethan Katsh and Orna Rabinovich-Einy. "The Internet of On-Demand Healthcare". In: *Digital Justice: Technology and the Internet of Disputes*. Oxford University Press, 2017, pp. 82–107. ISBN: 9780190464585, p. 87.

732 *See* Paolo Guarda and Rossana Ducato. "From electronic health records to personal health records: emerging legal issues in the Italian regulation of e-health". In: *International Review of Law, Computers & Technology* 30.3 (2016), pp. 271–285, p. 272.

733 *See* Giorgia Bincoletto. "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union". In: *Data & Policy* 2 (2020), pp. 1–11. DOI: 10.1017/dap.2020.2, p. 1, that reports the analysis of the EC European Commission. *Commission Staff Working document accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market*. Brussels: SWD (2018) 126 final. 2018.

734 One of the first dedicated communications from the EC on this topic is European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*. A detailed and recent report that assesses the impact of digital transformation in the EU is Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*.

The EU Action Plans on e-health began in the early 2000s[735]. The innovative healthcare policy plans aim to foster the adoption of e-health throughout the EU and remove barriers to its deployment[736]. The "transformation of health and care" policy plays an important role in the Digital Single Market programme. In particular, three priorities have been identified by the European Commission in the "Communication on Digital Transformation of Health Care in the Digital Single Market"[737]. Firstly, the EC calls for enabling EU citizens to access and share their health data securely across the Member States. Secondly, improving data quality for research purposes, disease prevention and to enable personalised healthcare shall be areas of action. Finally, the Commission asserts that further action at the EU level is crucial for developing e-health tools for citizens' empowerment and person-centred care[738].

Key points of these plans are the legal and regulatory issues. Directive 2011/24/EU on the application of patients' rights in cross-border healthcare has set up the e-Health Network in order to support healthcare providers and centres of expertise in the Member States[739]. This Network is a voluntary platform which connects national authorities responsible for e-health designated by the Member States[740]. The main goals of the

735 The first plan was adopted in 2004 with the European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*.

736 *See* European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century".

737 EC European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. European Commission. Brussels: COM (2018), 233 final. 2018.

738 These last three sentences appear in Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union".

739 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. O.J. L. 88, 4.4.2011.

740 Article 14 Directive 2011/24/EU. The rules for the Network are established by the EC European Commission. *Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C (2019) 7460)*. European Commission. Brussels: COM (2019), 7460 O.J. L. 270, 24.10.2019.

Network are providing guidance to Member States on digital health at several levels and facilitating the interoperability of the national ICTs systems and cross-border transferability of electronic health data in cross-border healthcare[741].

E-health tools and solutions include multiple and heterogeneous technologies that can be divided into different fields[742]:

– Telemedicine and telecare (e.g remote patient monitoring)[743];
– Clinical information systems (e.g. the systems connected in electronic health record systems)[744];
– Integrated information networks, e-referrals and e-prescribing[745];

2019. *See* also at <ec.europa.eu/health/ehealth/key_documents_en#anchor0>. Last accessed 06/10/2021.

741 Article 4 of European Commission, *op. cit.*

742 The classification is provided by Martin R. Cowie et al. "e-Health: a position statement of the European Society of Cardiology". In: *European heart journal* 37.1 (2016), pp. 63–66, p. 63. A technical literature review on e-health technologies is provided by Isabel CP. Marques and João JM. Ferreira. "Digital transformation in the area of health: systematic review of 45 years of evolution". In: *Health and Technology* (2019), pp. 1–12.

743 On this sector *see* with specific reference to EU, Guarda, "Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context"; Carlo Botrugno. "Telemedicine in daily practice: Addressing legal challenges while waiting for an EU regulatory framework". In: *Health Policy and Technology* 7.2 (2018), pp. 131–136; Catalina Ionescu-Dima. "Legal challenges regarding telemedicine services in the European Union". In: *eHealth: Legal, Ethical and Governance Challenges*. Springer, 2013, pp. 107–133. ISBN: 9783642224744. *See* also CL Wen. "Telemedicine, eHealth and Remote Care Systems". In: *Global Health Informatics*. Elsevier, 2017, pp. 168–194. ISBN: 9780128045916; Silvia Melchionna and Francesca Cecamore. "Le nuove frontiere della sanità e della ricerca scientifica". In: *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*. Giuffrè Francis Lefebvre, 2019, pp. 579–620. ISBN: 9788828809692, pp. 601–608. Madir, *Healthtech*, pp. 3–6 and pp. 354–373. Telemedicine has been defined by Guarda as a complementary tool that enhances the delivery of health services at a distance with the transmission of medical data and information.

744 On this specific category of e-health technology *see* further Section 3.4.1. As mentioned, Electronic Health Record (EHR) is the case study for DPbD.

745 *See* e.g. Patrick Kierkegaard. "E-prescription across Europe". In: *Health and Technology* 3.3 (2013), pp. 205–219. Kierkegaard defines e-prescription as a simple tool for generating a prescription electronically and sending it directly to a pharmacy from the point-of-care. It is also used in hospitals for managing the supply of medicines.

– Disease registries and systems used for education, public health, patient and disease- related behaviour, and healthcare management[746];
– Mobile health (e.g. mobile apps)[747];

746 Population-based registries are run by several countries. As an example, Scandinavian countries have a sophisticated statistical infrastructure for public health with multiple registries. *See* Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?", p. 80. On the Digital Youth Healthcare Registry in the Netherlands *see* Karolina La Fors-Owczynik. "Profiling 'Anomalies' and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime". In: *Under Observation: The Interplay Between eHealth and Surveillance*. Springer, 2017, pp. 107–138. ISBN: 9783319483429.

747 On mobile health from a legal perspective *see* e.g. Trix Mulder. "Health apps, their privacy policies and the GDPR". In: *European Journal of Law and Technology* 10 (1 2019); Madir, *Healthtech*, pp. 7–9; Eugenio Mantovani et al. "Towards a Code of Conduct on Privacy for mHealth to Foster Trust Amongst Users of Mobile Health Applications". In: *Data Protection and Privacy: (In)visibilities and Infrastructures*. Springer, 2017, pp. 81–106. ISBN: 9783319507965; EC European Commission. *Green paper on mobile Health*. European Commission. COM(2014) 219 final, 2014. The EC uses a WHO definition and states that mobile health covers "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices". From a technical perspective *see* e.g. Robert Istepanian, Swamy Laxminarayan, and Constantinos S Pattichis. *M-health*. Springer, 2006. ISBN: 9780387265599; Borja Martínez-Pérez, Isabel De La Torre-Díez, and Miguel López-Coronado. "Mobile health applications for the most prevalent conditions by the World Health Organization: review and analysis". In: *Journal of medical Internet research* 15.6 (2013), e120; Borja Martínez-Pérez, Isabel De La Torre-Díez, and Miguel López-Coronado. "Privacy and security in mobile health apps: a review and recommendations". In: *Journal of medical systems* 39.1 (2015), pp. 181–189; Waleed M Sweileh et al. "Bibliometric analysis of worldwide scientific literature in mobile-health: 2006–2016". In: *BMC medical informatics and decision making* 17.1 (2017), pp. 72–84; Achilleas Papageorgiou et al. "Security and privacy analysis of mobile health applications: the alarming state of practice". In: *IEEE Access* 6 (2018), pp. 9390–9403.

– Personalised health (e.g. wearable or implantable micro- and nano-technologies)[748];
– Big data (e.g. for predictive health), AI and Internet of Things[749].

E-health tools go beyond simply internet-based applications[750]. They can support, complement or substitute established health services, or they are

748 *See* e.g. from a legal perspective Bernd Blobel, DM. Lopez, and C. Gonzalez. "Patient privacy and security concerns on big data for personalized medicine". In: *Health and Technology* 6.1 (2016), pp. 75 – 81; and from a technical perspective Andrew G. Webb. "Mobile Health, Wearable Health Technology and Wireless Implanted Devices". In: *Principles of Biomedical Instrumentation*. Cambridge Texts in Biomedical Engineering. Cambridge University Press, 2018, pp. 235–270. ISBN: 9781316286210. For example, wireless implanted devices are pacemakers and cardiac re-synchronisation therapy devices. On biology-based personalised medicine *see* e.g. Lidia Becla et al. "Health technology assessment in the era of personalized health care". In: *International journal of technology assessment in health care* 27.2 (2011), pp. 118–126.

749 *See* e.g. from a legal perspective, Paolo Guarda. "'Ok Google, am I sick?': artificial intelligence, e-health, and data protection regulation". In: *BioLaw Journal-Rivista di BioDiritto* 15.1 (2019), pp. 359–375; Robin Pierce. "Machine learning for diagnosis and treatment: Gymnastics for the GDPR". In: *Eur. Data Prot. L. Rev.* 4 (2018), pp. 333–343; Agata Ferretti, Manuel Schneider, and Alessandro Blasimme. "Machine Learning in Medicine: Opening the New Data Protection Black Box". In: *Eur. Data Prot. L. Rev.* 4 (2018), pp. 320–332; Paolo Guarda and Livia Petrucci. "Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati". In: *BioLaw Journal-Rivista di BioDiritto* 2 (2020), pp. 425–446; Marta Arisi and Paolo Guarda. "Blockchain and eHealth: seeking compliance with the General Data Protection Regulation". In: *BioLaw Journal-Rivista di BioDiritto* 2 (2020), pp. 477–496; and from an interdisciplinary perspective, Chloé-Agathe Azencott. "Machine learning and genomics: precision medicine versus patient privacy". In: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376.2128 (2018), p. 20170350; Andreas Stylianou and Michael A. Talias. "Big data in healthcare: a discussion on the big challenges". In: *Health and Technology* 7.1 (2017), pp. 97–107. According to this last study, Big Data in health care is mainly produced by clinical data, pharmaceutical research, and patients' behaviour and sentiment data. The IoT has been added to the classification. On IoT for healthcare and e-consent *see* Yvonne O'Connor et al. "Privacy by design: informed consent and internet of things for smart health". In: *Procedia computer science* 113 (2017), pp. 653–658.

750 European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*, p. 4.

completely new[751]. Solutions operate both on a patient-to-doctor basis (e.g. telecare) and on a doctor-to-doctor basis (e.g. e-prescribing).

These digital innovations bring better information sharing and processing in the healthcare system and mediate the relationship between the individual as a patient and the healthcare provider (e.g physician, hospital). Thus, it has been argued that a risk of dehumanisation of the patient-physician relationship may exist because of the mediation of digital tools in healthcare provision[752]. However, technology should be a means for improving healthcare without compromising the fiduciary relationship based on respect and trust[753]. Some e-health technologies, such as mobile apps, may even change the role of the patient from a passive to a more active role[754]. In the e-health context, people want to be more involved in decisions and the asymmetry in knowledge between patients and physicians decreases[755]. Indeed, the patient's empowerment is a valuable contribution of digital health services[756].

---

751 *See* the classification in Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*, p. 30. Examples of supporting tools are personalised health systems. Telemedicine is complementary, whereas e-prescription is substituting. New tools are Big Data-based algorithms with treatment recommendations or medical chat-bots.

752 *See* Guarda, "Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context", pp. 10–11; Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*, p. 46; Guarda, "I dati sanitari", p. 615.

753 *See* for further discussion on trust in e-health, Penny Duquenoy, Nermeen Magdi Mekawie, and Mark Springett. "Patients, trust and ethics in information privacy in eHealth". In: *eHealth: Legal, Ethical and Governance Challenges*. Springer, 2013, pp. 275–295. ISBN: 9783642224744.

754 *See* the arguments of the European Commission in European Commission, *Green paper on mobile Health*, p. 5. On patient engagement and e-health technologies *see* the analysis of H. de Fátima Marin and Connie Delaney. "Patient Engagement and Digital Health Communities". In: *Global Health Informatics*. Elsevier, 2017, pp. 218–231. ISBN: 9780128045916.

755 European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*.

756 *See* Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*, p. 78. On the notion of patient empowerment *see* Guarda, "I dati sanitari", p. 592; Giuseppe de Vergottini and Carlo Bottari. *La sanità elettronica*. Bononia University Press, 2018. ISBN: 9788869233234, p. 80; Carla Faralli, Raffaella Brighi, Michele Martoni, et al. *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health*. G.

After the advent of e-health technologies, the more crucial and widely discussed challenges are privacy, and data protection and security of health data[757]. These aspects concern each category of e-health technologies mentioned above. Privacy and data protection concerns are related to the specific intimacy of health status, to the sensitiveness of the category of personal health data, and the security risk level that processing operations with HITs entails[758]. Privacy, data protection and security might be seen both as issues of e-health technologies and rights or obligations established by the law for minimising the risks for rights and freedoms of individuals.

The first concern is the privacy of e-health technology, meaning the protection against the potential impingement on the right to respect for private and family life in accordance with Article 7 of the EU Charter on Fundamental Rights, and Article 8 of the European Convention on Human Rights[759].

Giappichelli Editore, Torino, 2015. ISBN: 9788892100671, pp. 61–63. This expression has been used since the 90s and scholars have extensively discussed its evolution in the digital world.

757 In Kierkegaard, "E-prescription across Europe", p. 215, the most challenging aspects of e-health are privacy, confidentiality, data protection and liability. *See* also Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*, pp. 76, 81–83. The liability issue is a legal concern, and is related to the possible malfunctions of the systems and networks. According to the EC, the electronic commerce Directive applies to the provision of online health services. *See* further European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*, p. 14. So, this regulatory framework applies. Moreover, within the use of e-health technologies the traditional medical error may be related to a technological error. The legal basis for the civil liability should be found in many sources (e.g. product and service liability). On liability and e-health *see* the legal analysis by Isabelle Andoulsi and Petra Wilson. "Understanding liability in eHealth: Towards greater clarity at European Union level". In: *eHealth: Legal, ethical and governance challenges*. Springer, 2013, pp. 165–180. ISBN: 9783642224744.

758 For a systematic classification of the concerns *see* Aceto, Persico, and Pescapé, "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges", p. 144.

759 Article 8 of the Convention states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

Generally, a patient's medical condition (i.e. health status) is strictly personal and related to the intimate sphere of a specific individual. The body and mind of a natural person are central to personal life and to the sense of personal identity[760]. Health status affects several aspects of individual life, such as the ability to find a job or to conduct one's own business, or to obtain loans or insurance, and one's personal condition impacts the social dimension of everyday life[761]. Healthcare preserves individual dignity[762]. So, the interplay between dignity and privacy protects the right to self-determination of an individual body[763]. In the healthcare domain the right to privacy protects the freedom of choice and the trust relationship between doctor and patient[764]. The maintenance of a trustworthy relationship is fundamental to effective individual care and treatment[765].

Thus, privacy in the e-health context is a complex and multifaceted concept because it protects a wide spectrum of interests[766]. Various dimensions of privacy are implicated, such as bodily privacy or physical privacy (i.e. the control over one's body, and intimacy), decisional privacy (i.e. the ability to make decisions on a treatment without undue influence), and privacy of private space (e.g. in one's home)[767].

---

country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

760 *See* Elizabeth Wicks. "Electronic health records and privacy interests: The English experience". In: *eHealth: Legal, ethical and governance challenges*. Springer, 2013, pp. 57–76. ISBN: 9783642224744, p. 58.

761 *See* Giacomo Di Federico. "Access to Healthcare in the European Union: Are EU Patients (Effectively) Protected Against Discriminatory Practices?" In: *The Principle of Equality in EU Law*. Springer, 2017, pp. 229–253. ISBN: 9783319661377, p. 249.

762 *See ibid.*

763 Ludovica Durst. "Il trattamento di categorie particolari di dati in ambito sanitario". In: *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*. Giuffrè Francis Lefebvre, 2019, pp. 65–79. ISBN: 9788828809692, p. 71.

764 *See* the explanation of the concept and its relationship with human dignity in Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 162.

765 OECD, *OECD Recommendation on Health Data Governance*, Annex, 12.

766 *See* Robin Pierce. "Medical Privacy: Where Deontology and Consequentialism Meet". In: *The Handbook of Privacy Studies: an Interdisciplinary Introduction*. Amsterdam University Press, 2019, pp. 327–331. ISBN: 9789462988095, p. 32.

767 *See* e.g. the discussion related to mobile health in Maartje GH Niezen. "Unobtrusiveness in mHealth design and use: A systematic literature study". In: *Under Observation: The Interplay Between eHealth and Surveillance*. Springer,

It has been highlighted that confidentiality of medical conditions is instantiated in the Hippocratic Oath taken by physicians where it requires them to keep secret whatever they see or hear during the practices[768]. This professional secrecy protects the confidentiality of a patient's treatments in the patient-physician relationship[769]. This oath set the foundation of medical ethics[770].

Actually, medical confidentiality is a general principle in the healthcare domain, and is usually recognised by law as duty of confidentiality[771]. Confidentiality refers to the moral duty of non-disclosure of information shared in the patient-physician relationship[772]. The maintenance of confidentiality is then supported on deontological grounds[773]. For example, in the Italian Code of Medical Ethics the duty of confidence is set by Article 10, and is related to all information learned, and even the death of the patient does not end this duty[774].

The legal basis of duty of confidentiality is not easy to find because there is not a single provision, but multiple requirements in contract law, tort law, criminal law, and statutory obligations[775]. Health care actors have the attributes of fiduciary status in their relationships with patients that results in more than a contract or other form of legal liability for healing the indi-

---

2017, pp. 9–29. ISBN: 9783319483429, p. 2. The author argued that the use of m-health applications creates a high risk of surveillance since m-health devices and services are unobtrusive for users.

768 Duquenoy, Mekawie, and Springett, "Patients, trust and ethics in information privacy in eHealth", p. 281. *See* also Tamara K. Hervey and Jean V. McHale. *Health law and the European Union*. Cambridge University Press, 2004. ISBN: 9780511617553, p. 161. This article stresses that privacy and confidentiality are distinct notions in the healthcare domain especially. The Hippocratic Oath is translated in English as follows: "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart there from, which ought not to be noised abroad, I shall keep silence thereon, counting such things as sacred secrets".

769 *See* e.g. Mulder, "Health apps, their privacy policies and the GDPR".

770 Carissa Véliz. "Medical Privacy and Big Data". In: *Philosophical Foundations of Medical Law* (2019), p. 306, p. 308.

771 Wicks, "Electronic health records and privacy interests: The English experience", p. 58.

772 Véliz, "Medical Privacy and Big Data", p. 308.

773 *See* Hervey and McHale, *Health law and the European Union*, p. 162.

774 *See* Mario Tavani, Mario Picozzi, and Gabriella Salvati. *Manuale di deontologia medica*. Giuffrè Editore, 2007. ISBN: 9788814137297, p. 72.

775 Jonathan Herring. *Medical law and ethics*. Oxford University Press, 2016. ISBN: 9780198846956, p. 233.

vidual[776]. The duty of confidentiality arises from the mentioned attributes of fiduciary status and applies to professionals, hospitals and other health care providers[777]. Therefore, the breach of health confidentiality represents a cause of action in courts that is distinct from medical malpractice[778]. Moreover, the breach of confidentiality may be subject to professional disciplinary sanctions and criminal sanctions. It has been reported that breach of confidentiality is a criminal offence across many EU Member States[779].

In sum, confidentiality in healthcare is connected to the right to respect of private life[780]. It has been noted that privacy in the healthcare sector is necessary for guaranteeing an individual's dignity[781]. Since health is a central aspect of an individual's well-being, privacy and confidentiality are essential in a democratic society in order to protect people's private lives, their dignity, their right to not be discriminated against on the basis of their health status. The use of e-health technologies is challenging this guarantee since, now that medical information is collected in electronic form, more subjects may have access to health status, and may unlawfully share information with unauthorised third parties, or unauthorised parties may easily access to it illegally.

---

776 *See* Mark A. Hall. "Fiduciary Principles in Health Care". In: *The Oxford Handbook of Fiduciary Law*. Oxford University Press, 2019. ISBN: 9780190634100.

777 *See* Hall, *op. cit.*, p. 296.

778 *See ibid.* This statement is valuable for different legal frameworks.

779 *See* Hervey and McHale, *Health law and the European Union*, p. 16. As an example, the Italian Penal Code, Article 622 punishes anyone who, having knowledge for reasons of his or her profession reveals a secret without just cause, or uses it for his or her own or others' profit. The subject is punished if the act may result in harm with imprisonment of up to one year or a fine ranging from 30 to 516 euros. The offence is punishable on complaint by the injured person. In the Italian case law, the notion of profession is interpreted in a broad sense. *See* Laura Greco. "Il trattamento dei dati sanitari". In: *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*. Zanichelli, Torino, 2019, pp. 220–250. ISBN: 9788808820433, p. 232.

780 *See* Herring, *Medical law and ethics*, p. 277; Wouter Koelewijn. "Privacy from a Medical Perspective". In: *The Handbook of Privacy Studies: an Interdisciplinary Introduction*. Amsterdam University Press, 2019, p. 333. ISBN: 9789462988095.

781 *See* L. Palmieri. "Dai segreti alla riservatezza e poi al segreto". In: *Medicina Legale Quaderni Camerti* (XV 1993), p. 6; Licia 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* (3 2015), pp. 141–159, p. 9.

Arguably, the individual ethical and legal obligation of confidentiality upon the physician is no longer sufficient in the digital world[782]. It has been noted that medical confidentiality has been put under pressure because of technological innovations[783]. Hence, a well-known case of the European Court on Human Rights shows a bridge between the need to protect the respect of private life and confidentiality of health information, and the necessity to look at data protection issues when the context is the digital processing of personal health data.

In the case *I v. Finland* of 2008, the European Court on Human Rights recognised that medical confidentiality of health data is protected by Article 8 on private and family life of the Convention for the Protection of Human Rights and Fundamental Freedoms[784]. The applicant was a nurse affected by HIV who instituted a civil proceeding against the district health authority where she worked for an alleged failure to keep her patient record confidential, in violation of her right to respect for her private life[785]. After the Finnish judicial proceedings, the nurse applied to the Strasbourg Court for alleged violation of Article 8 of the European Convention by arguing that the measures to safeguard her right to respect for her private life had not been sufficient. The Court later held that there had been a violation of that Article by founding it applicable in the case because information related to patients belongs to their private life. Article 8 then entails a positive obligation to adopt measures for securing the respect of private life in every individual's relations[786]. The hospital, as the data controller, failed to secure the data against unauthorised and unlawful access. Indeed, the Court ruled that[787]:

> "the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the

782 Wicks, "Electronic health records and privacy interests: The English experience", p. 59.
783 Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 161.
784 The case of I v. Finland is Application no. 20511/03, Judgement of 17 July 2008.
785 The Judgement is available in the HUDOC database at <hudoc.echr.coe.int/eng>. Last accessed 06/10/2021.
786 *See* paragraph 36.
787 *See* paragraph 38.

> Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease".

The Court linked the protection of the respect for private life to the protection of medical information, which is fundamental in a democratic society[788]. The importance of this case has been recognised by the literature and prominent scholars even referred to it as an indirect reference to DPbD that created a state's positive obligation to secure the respect of Article 8 ECHR in order to ensure confidentiality of health data[789].

Indeed, data protection and security of personal health data represent significant concerns of e-health technologies. This category of data is sensitive in nature and requires a high level of protection[790]. According to the European Commission, effective data protection is a key driver for building trust in e-health[791].

In the e-health context, data quality should be a high priority of e-health systems[792]. Personal health data should be accurate and kept up to date – as in paper-based healthcare provision – in order to ensure efficient and high-quality treatment. Using adequate data available in e-health technology is important since inadequate data may cause medication and medical errors. So, data protection rules may even be a means for preserving healthcare efficiency and guaranteeing the accuracy of data.

---

788 In another prior case of the European Court on Human Rights, *Z. v. Finland*, the importance of the protection of health information was considered necessary for a democratic society. *See* case no. 22009/93, Judgement of 25 February 1997.

789 *See* Waldman, "Data Protection by Design? A Critique of Article 25 of the GDPR", p. 160; Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 110.

790 OECD, *OECD Recommendation on Health Data Governance*.

791 *See* European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century", p. 9.

792 *See* Katsh and Rabinovich-Einy, "The Internet of On-Demand Healthcare", p. 86.

Moreover, HIT security is a critical aspect[793]. The unauthorised access and misuse of health data are high risks in this sector[794]. In general, data breaches are typical security risks. Two of the main causes of data breach in the e-health care sector are hacking and maladministration[795]. In 2019, the EDPS reported that 90 % of the personal data breach security incidents in the EU were confidentiality breaches[796]. Actually, security is a huge problem in this context. Both technical and human factors are necessary for ensuring the confidentiality and integrity of health data[797].

It has been claimed that significant economic, psychological and social harms may be caused by unauthorised access or sharing of personal health data[798]. Actually, data about the health status can render the individual vulnerable in multiple ways[799]. As regards the economical level, the risk

793 *See* the security issue at European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*, p. 14.

794 *See* Ferretti, Schneider, and Blasimme, "Machine Learning in Medicine: Opening the New Data Protection Black Box", p. 331; and Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 161.

795 *See* two following examples. In Kierkegaard, "E-prescription across Europe", p. 216, the author reported the Virginia Department of Health's data breach. 35 million prescription records were downloaded and encrypted by a hacker who asked for a ransom of $ 10 million. In Leslie Stevens et al. "Dangers from within? Looking inwards at the role of maladministration as the leading cause of health data breaches in the UK". in: *Data Protection and Privacy: (In)visibilities and Infrastructures*. Springer, 2017, pp. 205–239. ISBN: 9783319507965, the authors reported some statistical data on health data breaches in the UK showing an increasing trend. The main cause is maladministration of healthcare providers. In this article the scholars classified the concepts that maladministration entails (i.e. careless and negligent abuse of data).

796 *See* EDPS European Data Protection Supervisor. *Annual Report 2019*. 2019, Section 3.2.3. In the same year the U.S. Department of Health & Human Services reported a massive and increased number of healthcare breaches. *See* the report's statistics on the website of the authority at <www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>. In 2019 the number of breaches increased by 37.4 %.

797 Duquenoy, Mekawie, and Springett, "Patients, trust and ethics in information privacy in eHealth", p. 280.

798 Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", p. 106. *See* also Véliz, "Medical Privacy and Big Data", pp. 310–313.

799 Pierce, "Medical Privacy: Where Deontology and Consequentialism Meet", p. 328.

is related to the possible advantages that insurance companies or private companies may obtain on acquiring such information and imposing specific unethical clauses targeted to the specific individual illness[800]. In addition, the employment and social sectors may be influenced by illegal access to health data. An individual may suffer employment and social exclusion if unauthorised information spreads (e.g. on chronic illness). Stigma, embarrassment and various forms of discrimination may result from an inappropriate protection of personal health data (e.g. in the case of a genetic risk of a disease)[801]. So, the knowledge of medical information may impact family relationships, career and work[802]. Indiscriminate and unauthorised use of this data affects the human person and his or her dignity[803].

---

800 Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", p. 106.

801 *See* Pierce, "Medical Privacy: Where Deontology and Consequentialism Meet", p. 328.

802 Duquenoy, Mekawie, and Springett, "Patients, trust and ethics in information privacy in eHealth", p. 281. *See* also Job Rimmelzwaan. "Use of a Wearable Device to Promote Healthy Behaviors Among Employees of a Small-to-Medium Enterprise in the Netherlands". In: *Under Observation: The Interplay Between eHealth and Surveillance*. Springer, 2017, pp. 59–69. ISBN: 9783319483429. The author presented an interesting case study in the context of employment in the Netherlands. For the promotion of healthy conditions in a company, employees' data were collected by the employer through wearable devices. This article demonstrated that people were not aware of the amount of data and of the sharing even though they trust their employer. The author pointed out that these data reveal more information on employees than what is necessary for a workplace. A case study on US employer-sponsored wellness programmes has shown the impact on informational privacy of this processing in the employment and insurance context. *See* Anna Slomovic. "eHealth and privacy in US employer wellness programs". In: *Under Observation: The Interplay Between eHealth and Surveillance*. Springer, 2017, pp. 31–58. ISBN: 9783319483429. Wellness programmes create the possibility to charge different insurance prices in accordance with employees' health. This study is strictly related to the complexity of the healthcare system in the US where employer health plans guarantee healthcare provision to workers. However, it has also shown the problematic use of health data collected by e-health technologies, such as mobile and wearable devices, for employment and insurance purposes. This system leads to an unprecedented surveillance and abusive scenario. The programmes are voluntary, but employees feel they are required by their employers to use them. As a result, health data are used to manipulate individuals' health-related behaviours.

803 On personal health data and human dignity *see* the constitutional perspective in Vergottini and Bottari, *La sanità elettronica*.

Therefore, e-health technologies should be highly secure for protecting the processing of personal health data. Data protection law supplements the legal and ethical duty of medical confidentiality[804]. The EU legal framework on data protection may mitigate all mentioned concerns since patients are data subjects and healthcare providers are usually data controllers that shall comply with the GDPR[805].

The right to respect for private life, the duties of confidentiality, and data protection laws set a variety of obligations for protecting personal health data. The obligations should be seen as aspects of the fair and legal treatment of a patient[806]. Organising the processing on the basis of legal protection by design is necessary for preventing abuse in the e-health environment[807]. From the beginning of EU Action Plans on e-health, PbD and PETs have been considered of paramount importance[808].

This section has presented the critical aspects of e-health technologies by highlighting their potential, too. The section that follows investigates the regulatory framework for the protection of personal health data at the EU level.

3.3 Regulatory framework for personal health data

The current legal framework in the EU for assessing the data protection issues mentioned is primarily the GDPR. The processing of personal health data by private or public healthcare entities in providing healthcare is subject to the General Regulation. However, other relevant provisions apply to this sector. In this section some general considerations on the regulatory framework for the processing of health data at the EU level will be presented.

---

804 Wicks, "Electronic health records and privacy interests: The English experience", p. 67.

805 *See* Ferretti, Schneider, and Blasimme, "Machine Learning in Medicine: Opening the New Data Protection Black Box", p. 331. The authors explained the opacity of AI systems in the medical field in light of the GDPR.

806 Wicks, "Electronic health records and privacy interests: The English experience", p. 76.

807 *See* the interesting discussion which follows Nissenbaum's theory of contextual integrity in Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 166.

808 *See* European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century", p. 9.

Personal data refers to all the information related to an identified or identifiable individual[809]. Personal data types can be divided into "common personal data", "personal data perceived as sensitive" by people and "sensitive data in the meaning of the GDPR"[810]. This last category is a subset of personal data that includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a natural person's sex life and sexual orientation[811]. In the GDPR, the legal framework establishes a general prohibition of processing personal data that are particularly sensitive by their nature since the context of their processing could create significant risks in relation to fundamental rights and freedoms[812]. Therefore, the processing is allowed in specific cases only. This approach was adopted under the DPD, too. The rationale of the general prohibition is minimising the significant risks that the processing of particular categories of personal data creates. In fact, these categories of data allow conclusions on the data subjects "that are linked to their fundamental rights and freedoms, such as freedom of thought, conscience and religion" or non-discrimination[813].

Personal health data are included in the list of special categories of data because they reveal information on the health status of the data subject that is linked to other rights and freedoms, such as the right to respect private and family life, and non-discrimination, as discussed above. Following the GDPR wording, data concerning health merits heightened protection. It should be pointed out that the GDPR sets specific provisions for the processing of special categories of data but leaves space to Member States to adapt the application of the rules at a national level[814]. Actually, the protection and improvement of human health are a competence of the Member States where the EU has the power to carry out actions

809 Article 4 GDPR. *See* Chapter 1, Section 1.1.

810 *See* Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA). Knowledge basis*, p. 2. In the second category the CNIL inserts social security number, biometric data and banking data.

811 Article 9(1) GDPR.

812 These are the words of Recital 51 GDPR.

813 *See* for each data category the risks defined by Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, pp. 110–111.

814 *See* Article 9(4) GDPR: "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".

to support, coordinate or supplement national actions[815]. Member States have the responsibility to define their health policies and organise and deliver health services and medical care, including the management of these services and the allocation of resources[816]. Nonetheless, protecting *health in all policies* is one of the transverse objectives of the EU[817]. In 2013, the EU even released a Decision on serious cross-border threats to health in order to coordinate the actions of Member States[818].

Under the DPD, many countries had sectoral legislation for the processing in the health care area[819]. Within the GDPR, the Member States can further define national rules on legal obligations related to personal health data, on tasks that should be carried out in the public interest, or on tasks that should be exercised under an official authority for private or public

---

815 Article 6(a) of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. On governance of health systems in the EU *see* Elias Mossialos et al. *Health systems governance in Europe: the role of European Union law and policy*. Cambridge University Press, 2010. ISBN: 9780511750496.

816 Article 168(7) of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union.

817 On health and the limited competences of the Union *see* Giacomo Di Federico and Stefania Negri. *Unione Europea e Salute. Principi, azioni, diritti e sicurezza*. Cedam Wolters Kluwer, 2020. ISBN: 9788813370886; Vergottini and Bottari, *La sanità elettronica*, pp. 102–105. On *health in all policies see* Mark Flear. *Governing Public Health: EU Law, Regulation and Biopolitics*. Bloomsbury Publishing, 2015. ISBN: 9781849462204; Tamara K. Hervey and Jean V. McHale. *European Union health law*. Cambridge University Press, 2015. ISBN: 9781107010499; Scott L. Greer et al. *Everything you always wanted to know about European Union health policies but were afraid to ask*. World Health Organization. Regional Office for Europe, 2014. ISBN: 9789289050272. On medical law at the EU and Member States' levels *see* the extensive research of the International Encyclopaedia of Laws in Herman Nys. *IEL Medical Law*. Kluwer Law International, 2020. ISBN: 9789065449436.

818 *See* Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC. O.J. L. 293, 5.11.2013. Article 16 of this Decision is dedicated to the protection of personal data and refers to the DPD by stating that: "In the application of this Decision, personal data shall be processed in accordance with Directive 95/46/EC and Regulation (EC) No 45/2001. In particular, appropriate technical and organisational measures shall be taken to protect such personal data against accidental or illegal destruction, accidental loss, or unauthorised access and against any form of illegal processing. (...)".

819 *See* Bart Custers et al. "A comparison of data protection legislation and policies across the EU". In: *Computer Law & Security Review* 34.2 (2018), pp. 234–243, p. 240.

health[820]. Moreover, national laws can derogate the general prohibition on the processing of health data where legislative measures are subject to "appropriate" and "suitable safeguards" and aim to protect a public interest in accordance with the principles of necessity and proportionality[821]. According to a report commissioned by the European Commission, most of the Member States provided national conditions and limitations on the processing of data concerning health[822].

In the public healthcare context, legislative derogation from the general prohibition of processing personal health data is generally allowed for health security, for monitoring and alert purposes, for preventing or controlling diseases and for other serious threats to public health[823]. According to Recital 52 of the GDPR, the purposes of the derogation may be public health, the management of healthcare services, or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The GDPR states that the expression of "public health", and

820 *See* further Section 3.3.2. In particular, Article 9(4) is the basis for the introduction of Member States' law on data concerning health.

821 Recital 52 GDPR.

822 *See* TIPIK, *Report on the implementation of specific provisions of Regulation (EU) 2016/679*, pp. 7–15: "Most of the Member States (BE, BG, CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT and RO) provide conditions/limitations on the processing of such data, while AT, CZ, DK, SE and SK do not provide any such specification clause". Moreover, "as regards data concerning health, the following conditions/limitations under Article 9(4) GDPR have been identified at national level: (i) listing the categories of persons who have access to such data (BE, BG, EL, ES, HU, LV, NL, PL); (ii) describing the function of those persons in processing such data (BE, LV); (iii) making the list of those persons available to the Data Protection Authority (BE); (iv) ensuring that those persons are subject to legal, statutory or other similar confidentiality obligations (BE, DE, ES, LT, PT); (v) allowing the processing only for specific purposes (EE, EL, FR, HR, HU, IE, LU, LV, NL, PL, PT, RO); (vi) requiring consent for processing to be in writing (EL, ES, FI, PT); (vii) requiring separate storage of data (ES) or limiting the time period (LV); (viii) requiring processing to be subject to compliance with specifications laid down by the national data protection authority (FR, IT) or to prior authorisation from the national data protection authority (FR, MT); and (ix) requiring anonymisation as a condition for access to data (PT). No Member States' legislation contained additional conditions or limitations with regard to the processing of genetic data, biometric data or data concerning health that could have the impact of restricting or prohibiting the free movement of personal data within the European Union".

823 *See* Recital 52 GDPR.

the underlying public interest, has been defined in Regulation (EC) No 1338/2008, whose Article 3 specifies that it means[824]:

> "All elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality".

So, the definition of this expression is broad and open to interpretation and shall be contextualised. Undoubtedly, the GDPR has given Member States freedom to restrict or extend the rules on personal health data processing[825]. In order to safeguard the interests of the natural person, the processing of personal data carried out for public health purposes shall be subject to suitable and specific measures and private third parties shall not process these data for other purposes[826]. Member States have this margin of manoeuvre for setting out specific processing situations without hampering the free and cross-border flow of personal health data[827]. Even though the wide margins of discretion of Member States could lead to a fragmentation of the EU legal framework and hinder the harmonisation of the GDPR, it is clear that the processing of data in the healthcare context involves cultural, social, ethical, political and economic factors, which undoubtedly differ from State to State[828]. It has been argued by

---

824 *See* Recital 54. Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work. O.J. L. 354, 31.12.2008.

825 The same approach was used in Data Protection Directive 95/46. *See* Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?", p. 85. An interesting general comment on the EU health policy and its fragmentation is Scott L. Greer. "Resistance in European Union health care policy". In: *The Routledge Handbook of European Public Policy*. Taylor & Francis Group, 2017, pp. 357–363. ISBN: 9781317404026. Member States resist EU healthcare policy and tend not to respond to EU initiatives.

826 Recital 54 GDPR refers to employers or insurance and banking companies.

827 Recital 53 states that: "Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data".

828 Greco, "Il trattamento dei dati sanitari", p. 225. A brief comparative analysis post GDPR may be found in Amram Denise. "Ricerca e protezione dei dati personali concernenti la salute: il tentativo di armonizzazione al livello europeo post GDPR e le interpretazioni offerte dai sistemi irlandese, belga, spagnolo e

Lynskey that the choice of the EU legislator was "to respect the divergent constitutional and cultural traditions of the Member States by allowing them to legislate to protect national sensitivities"[829]. Hence, a different data protection implementation for health data may persist across the EU, but harmonising national laws is of utmost importance for the Digital Single Market Strategy[830]. According to the report on the implementation of Article 9(4) GDPR, in 2021 no Member States' legislation restricted or limited the free movement of personal data within the EU[831].

For decades high importance has been assigned to cross-border healthcare[832]. Directive 2011/24/EU cited above establishes patients' rights that shall be guaranteed in cross-border healthcare[833]. The rationales of this act are ensuring a high-quality level of human health protection and trust in cross-border healthcare and promoting cooperation among Member States on healthcare provision[834]. A healthcare provider is any entity that legally provides healthcare within the territory of a Member State[835]. So, Directive 2011/24/EU applies to individual patients (i.e. "insured" people)

---

italiano". In: *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)* 1 (2019), pp. 211–223.

829 Lynskey, *The foundations of EU data protection law*, p. 73.

830 *See* Abedjan et al., "Data science in healthcare: Benefits, challenges and opportunities", p. 16; EDPS European Data Protection Supervisor. *Opinion 3/2020 on the European strategy for data*. European Data Protection Supervisor, 2020, p. 12. The EDPS pointed out "the need for further harmonization of data protection rules applicable to health data among the Member States".

831 *See* TIPIK, *Report on the implementation of specific provisions of Regulation (EU) 2016/679*, p. 9.

832 *See* from the European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*.

833 On this Directive *see* Paul Quinn and Paul De Hert. "The Patients' Rights Directive (2011/24/EU) – Providing (some) rights to EU residents seeking healthcare in other Member States". In: *Computer Law & Security Review* 27.5 (2011), pp. 497–502; Miek Peeters. "Free movement of patients: Directive 2011/24 on the application of patients' rights in cross-border healthcare". In: *European Journal of Health Law* 19.1 (2012), pp. 29–60; Hervey and McHale, *European Union health law*.

834 *See* Recitals 2, 5 and Article 1 of the Directive.

835 Article 3(g) Directive 2011/24/EU.

who decide to seek healthcare from a healthcare provider in a Member State other than the Member State of affiliation[836]. The Member State of treatment provides healthcare to the insured person, despite not being the country of residence of the person or the country where this person has the right to sickness benefits. Each Member State designates one or more national organisational contact points for cross-border healthcare[837].

Thus, European patients have the right to access healthcare when they are abroad, and the costs of the service will be reimbursed. They also have the right to access their electronic medical records, and therefore the collected data[838]. Anyway, the Directive specified that its application should not prejudice the protection of personal data pursuant to the data protection law[839]. The free and cross-border flow of personal health data, and therefore the cross-border transfer, is recognised by the Directive, but it should comply with data protection rules for safeguarding the fundamental rights to privacy and to data protection[840]. Previously, the EDPS supported the initiative in its opinion on the proposal[841]. The authority highlighted that the cross-border exchange of electronic data would have increased the risk of inaccurate or illegitimate data processing in the context of ICT applications, especially[842]. So, the EDPS stressed the importance of a privacy by design implementation of e-health technologies[843]. In previous studies on healthcare, it has been suggested that Directive

836 *See* Recital 11. According to Article 3, the Member State of affiliation is the country which has the competence of granting a prior authorisation to the treatment outside the Member State of residence, or in another Member State.

837 Article 6 establishes the rules for the national contact points.

838 Article 4(2)(f) states that "in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC". On this topic *see* further Section 3.4.3.

839 In Article 2 DPD is listed among other sources. Article 5 ensures the remote access to or a copy of patients' medical records "in conformity with, and subject to, national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC".

840 In particular, *see* Recital 25.

841 Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare. O.J. C. 128, 6.6.2009.

842 *See* paragraphs 20–23.

843 *See* paragraphs 27–34. Interestingly, the EDPS recommended the introduction of a specific Article on data protection and the incorporation of the notion of

2000/31/EC on electronic commerce may apply to e-health actors who act as information society services[844]. Following Recital 14 of this Directive, the EU data protection framework – i.e. DPD, and now the GDPR, and the e-privacy Directive – is fully applicable to information society services and the application of this Directive should be made in full compliance with the principles of data protection[845].

Another source of rule in the processing of health data at the EU level is Regulation 536/2014 on clinical trials of medicinal products for human use[846]. Generally, clinical studies and trials are investigations intended to verify the effects or reactions of medical products or therapeutic strategies. Data subjects' personal health data are processed to test the products in the course of a scientific research activity. According to Recital 161 of the GDPR, the relevant rules of Regulation 536/2014 shall apply[847]. Since clinical trials involve the intimate sphere of individuals, they should respect "the rights, safety, dignity and well-being of subjects", who have "priority over all other interests", and "the data generated should be reliable and robust"[848]. Thus, the GDPR applies within the framework of this Regulation[849].

The same healthcare providers defined by Directive 2011/24/EU, including hospitals and private clinics, shall also comply with the national implementations of Directive 2016/1148 on measures for networking and

---

privacy by design. However, the legislative process of the Directive did not take into account these two recommendations.

844 *See* Mossialos et al., *Health systems governance in Europe: the role of European Union law and policy*, p. 566; Botrugno, "Telemedicine in daily practice: Addressing legal challenges while waiting for an EU regulatory framework". *See* the definition of "information society service" in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). O.J. L. 178, 17.7.2000.

845 On this Directive *see* also Arno R. Lodder. "European Union E-Commerce Directive-Article by Article Comments". In: *Guide to European Union Law on E-Commerce*. Vol. 4. Elgar Commentaries series, 2017, pp. 15–58. ISBN: 9781785369339.

846 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. O.J. L. 158, 27.5.2014.

847 *See* Recital 161.

848 Recital 1 of the Regulation 536/2014.

849 Regulation 536/2014 still refers to the DPD at Recital 76 and Article 93, but the DPD has been repealed by the GDPR.

systems security[850]. The processing of personal data in this framework shall be carried out in accordance with the GDPR[851].

Moreover, it should be mentioned that in 2017 two Regulations on *in vitro* diagnostic medical devices and on medical devices provided the rules concerning these products and established the creation of the comprehensive electronic database "Eudamed"[852]. These acts follow the medical directives that aimed to harmonise the rules on the free circulation of medical devices in the EU[853]. Once again, the GDPR applies to the processing of personal health data carried out in Member States pursuant to these regulations[854].

---

850 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. O.J. L. 194, 19.7.2016. On this directive *see* Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation". In: *Computer Law & Security Review* 35.6 (2019), p. 105336.

851 Actually, Article 2 of this Directive refers to the DPD, which has been repealed by the GDPR.

852 The two Regulations are: Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. O.J. L. 117, 5.5.2017; and Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. O.J. L. 117, 5.5.2017. Due to the COVID-19 emergency this Regulation has been amended by Regulation (EU) 2020/561 of the European Parliament and of the Council of 23 April 2020 amending Regulation (EU) 2017/745 on medical devices, as regards the dates of application of certain of its provisions. O.J. L. 130, 24.4.2020. According to the Regulation (EU) 2017/745, the expression "medical device" means "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability; investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations".

853 *See* Mossialos et al., *Health systems governance in Europe: the role of European Union law and policy*, p. 568. Madir, *Healthtech*, pp. 25–28 and pp. 53–79.

854 *See* the reference made by the Regulations to the GDPR at Article 110 for Regulation 2017/745 and at Article 103 for Regulation 2017/746.

From a European perspective, a legal framework in this domain is the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereafter: "Convention 108") which is the "only legally binding multilateral agreement in the field of personal data protection"[855]. The Convention aims to protect Article 8 ECHR and act as a global information privacy standard[856]. EU data protection law has been influenced by the Council of Europe's Convention 108 and these two legal frameworks follow the same logic[857]. The Convention, which was amended in 2018, and then signed by all EU Member States mandates some principles, rules and safeguards to be implemented in domestic law[858]. It is worth mentioning that even the

855 This wording has been used by the European Commission in EC European Commission. *Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*. European Commission. Brussels: COM (2018), 449 final. 2018. On the relevance of the CoE Convention *see* Paul de Hert and Vagelis Papakonstantinou. "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition". In: *Computer Law & Security Review* 30.6 (2014), pp. 633–642.

856 *See* the comment by Hert and Papakonstantinou, *op. cit.*, p. 641.

857 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*; Mulder, "Health apps, their privacy policies and the GDPR". On the relevance of the Convention *see* e.g. Paul de Hert and Vagelis Papakonstantinou. "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition". In: *Computer Law & Security Review* 30.6 (2014), pp. 633–642; European Commission, *Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*. On the territorial and functional scopes *see* Jorg Ukrow. "Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108". In: *Eur. Data Prot. L. Rev.* 4 (2018), pp. 239–247.

858 The authorisation to sign was provided by Council Decision (EU) 2019/682 of 9 April 2019 allowing Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. O.J. L. 115, 2.5.2019.

Modernised Convention 108 considers medical data a special category of data[859]. This Convention contains similar safeguards as the GDPR[860].

The Council also issued three specific and relevant documents on health data processing. Three recommendations are specifically devoted to medical data and how the processing should be carried out. The recommendations are legal instruments of the Council of Europe that are not binding for the Council of Europe's member states, but are aimed at providing policy frameworks and harmonising domestic law to ensure a higher level of protection of rights[861].

Firstly, Recommendation No. R(97) 5 on the protection of medical data of 13 February 1997 specifically applies to the collection and automatic processing of medical data – i.e. "all personal data concerning the health of an individual", including "data which have a clear and close link with health as well as to genetic data" – in the absence of a national law that provides other appropriate safeguards[862]. According to this Recommendation, the processing of medical data should be carried out only by healthcare professionals, or by subjects working on their behalf. Other controllers should be subject to equal rules of confidentiality or effective safeguards at the national level. As far as this study is concerned, this Recommendation sets the principles for the processing, the legitimate basis, the information that the data subject should receive, the rights of the data subject and the security safeguards that should be taken to protect medical data[863].

Secondly, Recommendation CM/Rec (2016) 8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, of 26 October 2016, is aimed at ensuring the respect for the fundamental

859 *See* Article 6 Convention 108. For the text of the Convention *see* <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>. Last accessed 06/10/2021.

860 *See* the useful comparison by Ukrow, "Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108".

861 For the legal status of the Council's recommendations *see* Stefanie Schmahl and Marten Breuer. *The Council of Europe: its law and policies*. Oxford University Press, 2017. ISBN: 9780199672523, p. 763; Florence Benoît-Rohmer, Heinrich Klebes, et al. *Council of Europe law: towards a pan-European legal area*. Council of Europe Publishing, 2005. ISBN: 9789287155948, p. 107.

862 On a legal analysis of this Recommendation *see* Trix Mulder. "The Protection of Data Concerning Health in Europe". In: *Eur. Data Prot. L. Rev.* 5 (2019), p. 209, pp. 213–215.

863 *See* further the text of the Recommendation.

rights of individuals without discrimination in the context of insurance contracts[864]. This recommendation is relevant for the e-health sector since the processing of data for insurance purposes implies high risks for the rights of the data subject, as explained above[865].

Thirdly, Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data of 27 March 2019 applies to the processing of personal health data in the public and private sectors. This document stresses the importance of taking steps to better protect health-related data. It is applicable to the exchange and sharing of health-related data carried out by e-health technologies. This Recommendation lists the principles concerning data processing, by including the same principles of the GDPR with some additions[866]. In addition to transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, security, accountability, and storage limitation[867], the Committee specifies that personal health-related data "should, in principle and as far as possible, be collected from the data subject", unless the "data subject is not in a position to provide the data and such data are necessary for the purposes of the processing"[868]. The security principle requires the implementation of appropriate security measures by taking into account "the latest technological developments", "the sensitive nature of health-related data and the assessment of potential risks" in order to prevent security risks[869]. According to the Recommendation, the controller should take into account all the mentioned principles by default, incorporate the rights from the design of e-health technologies, and regularly carry out an impact assessment of the potential impact of the processing of data[870]. This is a direct reference to a DPbD implementation in the healthcare domain. Furthermore, whenever the controller is not a health professional, the processing is subject to rules of confidentiality and security that ensure a level of

---

864 *See* the General Provisions of the Recommendation.

865 *See* also Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 337.

866 *See* Chapter II – Legal conditions for the processing of health-related data paragraph 4.

867 This principle has been established in paragraph 10.

868 *See* paragraph 4(d).

869 *See* paragraph 4(f). *See* also paragraph 13 on security. The Recommendation even refers to conditions for securing the e-health system's availability, integrity, and auditability, the storage and sharing of data, and the access mechanism. These are all aspects that a DPbD implementation should take into account. *See* further Chapter 6.

870 *See* paragraph 4.2.

protection equivalent to the one imposed on health professionals[871]. The document recommends the legitimate basis of processing[872], some specific safeguards for genetic data and for the sharing and communication of data[873]. The information to be provided and the rights and obligations are equivalent to the elements of the GDPR, but the Recommendation presents fewer details.

The focus of this research is on the GDPR, and its DPbD obligation. The next subsections will now focus on this framework by providing the definition of personal health data, the legal grounds for their processing and the other relevant legal requirements that are applicable in the context of e-health and useful for a DPbD implementation.

3.3.1 The definition of personal health data

The definition of personal health data and the delimitation of its scope have raised doubts of interpretation[874]. This section attempts to provide guidance on this definition.

According to Article 29 Working Party, the category of health-related data is one of the most complex of sensitive data since it is often associated with serious privacy infringements[875]. Following the WHO's definition of health, this concept refers to the complexity of individual well-being at physical, mental and social levels[876].

The DPD mentioned data concerning health in the category of sensitive data, without defining it. Scholars argued that the absence of a normative definition was justified by the intention to leave the practitioner free to

871 *See* paragraph 4.4.
872 *See* for a comparison with the GDPR Section 3.3.2.
873 *See* paragraphs 7–9.
874 *See* Guarda, "I dati sanitari", p. 595; Mulder, "The Protection of Data Concerning Health in Europe"; Koelewijn, "Privacy from a Medical Perspective", p. 336. Lee A. Bygrave and Luca Tosoni. "Chapter I General principles (Articles 1–4). Article 4(15). Data concerning health". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 215–224. ISBN: 9780198826491.
875 WP29 Article 29 Working Party. *Advice paper on special categories of data ("sensitive data")*. Ref. Ares (2011) 444105, 20.04.2011. 2011, p. 10.
876 *See* the introductory remarks of this Chapter.

decide from time to time which information falls under the scope of the rules on health data[877].

In the judgement *Criminal proceedings v. Bodil Lindqvist* the Court of Justice argued that the notion of personal data concerning health should include a "reference to the fact that an individual has injured her foot and is on half-time on medical grounds"[878]. The judgement refers to a preliminary ruling of the Swedish Göta Court of Appeal. The criminal proceeding was opened against Mrs. Lindqvist, who was a volunteer in a parish of the Swedish Protestant Church and published on her website personal data of a number of people working with her. Mrs. Lindqvist was convicted for processing sensitive data without authorisation from the DPA. This case was issued under the DPD, but it is still relevant for the definition of data concerning health since the CJEU pointed out that a broad interpretation of this expression shall be given in order to include information concerning all aspects, both physical and mental, of the health status of an individual[879]. The ruling of the Court shows the difficulties surrounding the concept of health data since the concrete context defines more than a given list on information which is sensitive[880]. Interpreters should adopt a teleological approach.

Article 29 Working Party then analysed the notion under the DPD[881]. The term "health data" should be interpreted in a broad sense. The authority presented several examples of information concerning health in the

877 *See* Fausto Caggia. "Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario". In: *Il codice del trattamento dei dati personali. Giappichelli, Torino* 8 (2007), p. 405, p. 407.

878 Case C-101/01, Criminal proceedings against Bodil Lindqvist. Judgment of 6 November 2003. *See* also Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 96.

879 *See* paragraph 50.

880 *See* the comment by Ian Lloyd. *Information technology law*. Oxford University Press, 2020. ISBN: 9780198830559, p. 42; and Peter Carey. *Data protection: a practical guide to UK and EU law*. Oxford University Press, 2018. ISBN: 9780198815419, p. 68, which specifies that personal data may be seen in context in order to determine whether or not they are actually special data. Other case law on sensitive data is reported by Ludmila Georgieva and Christopher Kuner. "Chapter II Principles (Articles 5–11). Article 9 Processing of special categories of personal data". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 365–384. ISBN: 9780198826491, pp. 372–373.

881 *See* WP29 Article 29 Working Party. *Working Document on the processing of personal data relating to health in electronic health records (EHR)*. WP131 2007/en. 2007, p. 7.

legal sense, such as data on consumption of medicinal products, alcohol or drugs, genetic data, and any other data contained in the medical documentation of the treatment. In 2011 in order to clarify the scope of the notion in relation to lifestyle and well-being apps, WP29 pointed out that "medical data" are uniformly considered "health data", meaning "data about the physical or mental health status of a data subject that are generated in a professional medical context"[882]. All data relating to diagnosis, diseases, disabilities, medical history and clinical treatment should be included in this definition.

However, according to WP29, the expression "health data" is broader than the term "medical data" since it encompasses other related information, such as data about smoking and drinking habits, data on allergies, membership in a patient support group, information on illness in an employment context, data used in an administrative healthcare context, data about the purchase of medical products, devices and services when health status can be inferred from this information[883]. Merely lifestyle data, such as the number of steps during a daily walk, is "raw data" and is not "health data" in the legal sense. It should be noted that a grey area may remain since raw information can be often combined, and then conclusions on medical risk of the individual can be inferred, irrespective of whether they are accurate (e.g. using blood pressure and sex, age, etc.). According to WP29, these conclusions shall be considered "health data"[884].

Compared to the DPD, in Article 4 the GDPR clarifies the concept by expanding the definitions with health-related specifications on "genetic data" and "data concerning health"[885]. Commentators highlight that these

882 *See* WP29 Article 29 Working Party. *ANNEX – health data in apps and devices*. Annex to the letter of 5.2.2015, 2015.

883 Article 29 Working Party, *op. cit.*, p. 2.

884 Article 29 Working Party, *op. cit.*, p. 5. *See* also the commentary by Caterina Del Federico and Anna Rita Popoli. "Le definizioni". In: *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*. Zanichelli, Torino, 2019, pp. 63–88. ISBN: 9788808820433, p. 78.

885 For a brief comparison *see* Durst, "Il trattamento di categorie particolari di dati in ambito sanitario", pp. 66–67. The GDPR also adds the definition of "biometric data", which means any "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". *See* Article 4 GDPR (14) GDPR. On biometric data *see* e.g. Els J. Kindt. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Springer Netherlands, 2013. ISBN: 97894007752.

specifications reflect the growing importance of e-health at the EU level in recent years[886]. So, it has been pointed out that now the data relating to health are defined and detached from the more general and generic interpretation previously adopted by authorities and legal practitioners[887].

The first term of "genetic data" is a special sub-category of data concerning health and refers to "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question"[888]; whereas the second term of "data concerning health" has been framed as follows[889]:

> "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".

Recital 35 further explains which data are related to health status by adding the timing dimension, extending the scope of the definition, and by stating that:

> "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject".

---

886 *See* e.g. Durst, "Il trattamento di categorie particolari di dati in ambito sanitario", p. 72.

887 *See* Guarda, "I dati sanitari", p. 597.

888 Article 4(13) GDPR. Moreover Recital 35 also specifies that "genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained". On genetic data *see* e.g. Guarda, *op. cit.*, pp. 621–625; Mahsa Shabani and Pascal Borry. "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation". In: *European Journal of Human Genetics* 26.2 (2018), pp. 149–156; Kärt Pormeister. "The GDPR and Big Data: Leading the Way for Big Genetic Data?" In: *Annual Privacy Forum*. Springer. 2017, pp. 3–18; Mark Taylor. *Genetic data and the law: a critical perspective on privacy protection*. Vol. 16. Cambridge University Press, 2012. ISBN: 9780511910128; Laurie Graeme. *Genetic privacy: a challenge to medico-legal norms*. Cambridge University Press, 2002. ISBN: 0521660270.

889 Article 4(15) GDPR.

Not only information on the past, but also on the future health status should be considered personal data concerning health. The same Recital adds further interpretation and specifies some information which shall be included in the notion. It can be listed as follows:

- "information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person", which refers to the cross-border provision of healthcare described above;
- "a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes", which refers to administrative data used for healthcare purposes;
- "information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples", which is the inferred data, or the laboratory data, or genetic data inferred from biological sample, such as chromosomal, DNA or RNA analysis;
- "any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test", which is the traditional notion of "medical data".

In this definition the GDPR explicitly includes the data processed under the regulatory framework outlined above: Directive on the cross-border healthcare, and the two Regulations on *in vitro* diagnostic medical devices and on medical devices. As a result, the legal system on data protection is consistent. The GDPR applies to any personal data concerning health that is processed under the EU law. It refers to genetic information and biological samples, too. Moreover, as mentioned in the previous Chapter, it should be recalled that the Regulation 2018/1725 applies to the processing carried out by EU institutions, bodies and agencies. This Regulation uses the same definitions of genetic data, biometric data, and data concerning health[890].

Following the GDPR wording, it can be noted that the definition of data concerning health is broad[891]. It is now explicitly broader than simply

890 Article 3 lists all the definitions.

891 *See* e.g. Durst, "Il trattamento di categorie particolari di dati in ambito sanitario", p. 73; Koelewijn, "Privacy from a Medical Perspective", p. 337.

"medical data" and is applicable at the EU level. The explicit reference to administrative data related to health (i.e. the "number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes") better specifies the concept by following the previous interpretations of WP29, DPAs and scholars[892]. The definition of personal data concerning health embeds both the strictly care level and the services that it includes. For the purpose of this book, the term "personal health data" means "data concerning health" in the meaning of the GDPR.

Recital 35 is more comprehensive than Article 4, but it does not define whether or not other types of "quasi-health" data (e.g. lifestyle and well-being data) are considered health data[893]. It may be argued that the future dimension of the definition embeds the data inferred with predictive analysis tools[894]. The legal notion surely includes the data related to any health status, the information collected in the cross-border exchange of health data, on clinical studies and trials, and all the information on any medical treatment or examination regardless of the sources. Hence, personal data which have a clear link with the description of the health status and the medical treatment of a person shall fall within the definition of Article 4 GDPR.

However, health apps or wearable devices can frequently generate inferences about health conditions or risk of illness[895]. Some prominent scholars tried to delimit the boundaries of health data using a computational approach based on the sensitivity of the data[896]. According to Malgieri and Comandé, raw data can be divided into "received data" (i.e. data provided by the data subject) and "observed data" (i.e. data collected through the system with sensors), whereas "complex data" consists of "inferred data" (i.e. descriptive data inferred by the controller containing different information, such as the health status) and "predicted data" (i.e.

892 In Melchionna and Cecamore, "Le nuove frontiere della sanità e della ricerca scientifica", p. 581, the author referred to several opinions of the Italian DPA. For the interpretation of the scholars *see* the discussion in Guarda, "I dati sanitari", pp. 593–597.

893 Mantovani et al., "Towards a Code of Conduct on Privacy for mHealth to Foster Trust Amongst Users of Mobile Health Applications", p. 90.

894 In Koelewijn, "Privacy from a Medical Perspective", the author mentions big data technologies generally.

895 *See* Gianclaudio Malgieri and Giovanni Comandé. "Sensitive-by-distance: quasi-health data in the algorithmic era". In: *Information & Communications Technology Law* 26.3 (2017), pp. 229–249, p. 230.

896 *See* Malgieri and Comandé, *op. cit.*

information on the future health status)[897]. It is necessary to determine whether or not data not directly related to the health status, but capable of revealing the future status (e.g. observed data on number of steps walked per year or inferred data on sexual habits), are health data. These scholars concluded that complex information should be considered "quasi-health" data since it is nearly as sensitive as health data, and it should be selected on a case-by-case basis in accordance with the two variables of "intrinsic sensitiveness" and "computational distance"[898]. The status of "quasi-health" data is comparable to sensitive data. Within this framework, it should be easily determined which information falls under the legal notion of health data following a case-by-case approach based on a strict methodology.

The notion resulting from the GDPR is consistent with the OECD's international definition of "personal health data", that is "any information relating to an identified or identifiable individual" (e.g. personal data) "that concerns their health, and includes any other associated personal data"[899]. The timing of health status indicated in the GDPR has also been used for the CoE definition in the Recommendation CM/Rec (2019) 2, where health-related data are "all personal data concerning the physical or mental health of an individual, including the provision of health-care services, which reveals information about this individual's past, current and future health"[900]. It has been argued that the use of the term "information" implies that the data itself is not protected, unless it is used to gain information on an individual's health status[901].

Finally, it should be noted that the literature and regulatory frameworks may use the notion of "particularly sensitive health data", which consists

---

897 The definitions are summarised from the description in Malgieri and Comandé, *op. cit.*, p. 232. *See* also Giovanni Comandé and Giulia Schneider. "Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data'". In: *European Journal of Health Law* 25.3 (2018), pp. 284–307.

898 The proposed definition of "quasi-health" data is "information apparently not related to health conditions but which, if combined with biographical data (age, sex, etc.) and/or with statistical or biological studies, enables inference or prediction of individuals' health conditions with a certain degree of plausibility". The computational distance is related to the level of effort required to infer the information. Intrinsic sensitivity is a static variable, whereas computational distance is a dynamic variable, and they are inversely proportional. *See* Malgieri and Comandé, "Sensitive-by-distance: quasi-health data in the algorithmic era".

899 OECD, *OECD Recommendation on Health Data Governance*, p. 4.

900 *See* Chapter I – General Provision paragraph 2 and 3 of the Recommendation.

901 *See* Mulder, "The Protection of Data Concerning Health in Europe", p. 212.

in a sub-set of personal health data whose processing requires additional safeguards provided by national law[902].

Given the notion of personal health data and recalling the existence of a general prohibition on processing this data, in the next section the legitimate grounds for the processing of this category of data will be analysed in detail.

3.3.1 The legal grounds for processing

Generally, the legal grounds for the processing of sensitive data are narrower than the grounds for common personal data. The DPD established a general prohibition on processing sensitive data that has proven to be successful since it provided for few exceptions and several additional safeguards[903]. The advantages of this approach were summarised by Article 29 working Party as follows. The DPD gave a "strong political signal that the processing of sensitive data is generally prohibited" and it harmonised the categories of sensitive data providing legal certainty for data controllers on the limits[904]. At the same time, the complete harmonisation of the exceptions was not achieved in national implementing legislation[905].

Under the GDPR, the EU legal framework is better harmonised, but, as mentioned, Member States still have room to manoeuvre. Thus, it has been claimed that it is nearly impossible to carry out a real unification of the rules on the processing of health data at the EU level[906]. However, according to Recital 53 of the GDPR, the processing of personal data for health-related purposes should be allowed only in the context where it is "necessary to achieve those purposes for the benefit of natural persons and

902 *See* e.g. 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", which reports the notion existing in the Italian framework. Particularly sensitive data are HIV health status, abortion, sexual assault, drug abuse, and anonymous birth. *See* also Guarda, "I dati sanitari".

903 *See* the comments of Article 29 Working Party, *Advice paper on special categories of data ("sensitive data")*, p. 13.

904 *Ibid.*

905 *Ibid.*

906 Guarda, "I dati sanitari", p. 600.

society as a whole"[907]. So, the processing of personal health data may refer both to the individual interest and to public interests.

The enumeration of the legal grounds of processing, i.e. the exceptions to the general prohibition listed by Article 9 of the GDPR, is exhaustive. They largely overlap with the limits of the DPD[908]. However, as mentioned, Member States' laws "may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health"[909].

Firstly, article 9(2)(h) explicitly allows for processing personal health data when the purposes are preventative or occupational medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services on the basis of Union or Member State law or pursuant to a contract with a health professional[910]. In these cases, the processing shall be carried out by a healthcare professional who is subject to a duty of secrecy or confidentiality under Union or Member State law or other national provision[911]. The collected personal health data shall be necessary

907 Recital 53 GDPR. The Recital lists some contexts where this achievement is considered appropriate for society, which are: "the management of health or social care services and systems" that include several scenarios of "processing by the management and central national health authorities of such data for the purpose of quality control, management information" and of "the general national and local supervision of the health or social care system" and of "ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes"; "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", which are "based on Union or Member State law" and meet "an objective of public interest"; and "studies conducted in the public interest in the area of public health".

908 *See* further discussion at the end of this section.

909 Article 9(4) GDPR.

910 The grounds have been summarised in this way by Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 336. The paragraph of the GDPR states: "(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

911 *See* Article 9(3) GDPR: "3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules

for the treatment. As a result, it has been argued that healthcare providers should always check whether the collected personal health data is in reasonable proportion to the goal of one of the purposes listed above and whether less data could be sufficient to achieve it[912].

This legitimate ground may be called the "healthcare exception" and it is similar to a provision of the DPD[913]. Under the DPD, it has been claimed that this exception, restricted to a specific target of subjects, was difficult to apply in the healthcare sector since it was often not clear who belongs to the category of health professionals in practice or to the group of persons obliged to equivalent secrecy duties[914]. To interpret the notion of professional it is useful to look at other legislation applicable in the health sector. According to Article 3 of Directive 2011/24/EU the term "health professional" refers to a natural person who is "a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC on the recognition of professional qualifications", or "another professional exercising activities in the healthcare sector which are restricted to a regulated profession" as defined by the same Directive, or "a person considered to be a health professional according to the legislation of the Member State of treatment"[915]. So, it can be argued that the exception of the GDPR refers to this category of subjects whose professional status is recognised by Union or Member State law, and to other categories subject to an equivalent secrecy under the law (i.e. non-medical professional).

---

established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies".

912 *See* Koelewijn, "Privacy from a Medical Perspective", p. 339.

913 In this regard, the Directive at Article 8(3) stated that the prohibition on processing sensitive data "shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy".

914 Article 29 Working Party, *Advice paper on special categories of data ("sensitive data")*, p. 9. Article 29 Working Party called for a revision of the DPD for the broad term "health professional".

915 The definition refers to Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications. O.J. L. 255, 30.9.2005. For example, in Chapter III, Section 2 is entirely dedicated to doctors of medicine.

The rationale underlined by this first exception is avoiding the compulsory collection of patient's consent in order to simplify and facilitate the performance of healthcare services[916]. In addition, any errors in the collection of consent does not affect the proper performance of activities of higher interest, such as those related to health protection since consent is not necessary[917]. As a result, when processing is instrumental to the provision of healthcare, the controllers do not need to collect consent and their operations are simplified. Undoubtedly, the general duty of confidentiality provided by law remains. As mentioned above, this duty is even covered by criminal law provisions in some countries[918]. So, the breach of this duty of confidentiality may be punished with criminal sanctions, and the duty of secrecy is usually provided by physicians' codes of medical ethics.

It should be pointed out that this "healthcare exception" never applies to the insurance sector. Insurance companies that are not healthcare providers process health data since this information is a necessary prerequisite for concluding and performing a health insurance contract. Therefore, the processing for insurance purposes collects personal health data, but it shall use another legitimate ground that is the consent of the data subject. It has been claimed that this consent does not often meet the legal requirements of explicit, informed and free consent due to the use of blanket declarations which cover numerous forms of data processing[919]. Anyway, another legal ground listed as an exception in Article 9 GDPR is the consent of the data subject to the specific processing and related purpose, where consent is explicit[920].

As regards explicit consent, it is not necessarily written since the requirement constrains the purpose of the consent, but the form of expression is free, and can even be oral or expressed though behaviour[921]. So, the

916 *See* Greco, "Il trattamento dei dati sanitari", p. 228.

917 *See ibid.*

918 *See* Hervey and McHale, *Health law and the European Union*, p. 162.

919 Article 29 Working Party, *Advice paper on special categories of data ("sensitive data")*, p. 9. Article 29 Working Party called for a revision of this aspect, too.

920 Article 9(2)(a) provides that the processing is allowed when "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject".

921 Selvaggia F. Giovannangeli. "L'informativa agli interessati e il consenso al trattamento". In: *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*. Giuffrè Francis Lefebvre, 2019, pp. 100–141. ISBN: 9788828809692, p. 117.

individual shall explicitly and clearly express his or her will to grant permission for the processing and the controller has the burden of proof that the consent meets the GDPR requirements[922]. Although the form of consent is free, the controller is accountable for proving the receipt of the express statement of consent[923]. The consent shall respect the requirements of Article 7 and 8 GDPR – i.e. it shall be freely-given, specific, informed and unambiguous – and it shall explicitly refer to the personal health data concerned[924]. Union or Member State law could limit the applicability of this exception to specific categories of sensitive data. It has been pointed out that it is unlikely that such prohibition will be created by the EU since the EU has limited competence in this area[925]. Instead, the Member States can provide particular cases when the prohibition of processing health data may not be lifted by the consent of the data subject.

Explicit consent is required in circumstances where the data subjects are testing pharmaceutical products or medical devices and their personal genetic, health and related data are useful for the test phases and clinical trials[926]. The data collected in clinical trials can also be considered for secondary scientific research purposes. Regulation 536/2014 on clinical trials of medicinal products for human use requires the consent of the data subject for processing in the clinical study and trial, and also for the use of data outside the protocol of the clinical trial. The subject has the right to withdraw that consent at any time. As will be explained in the following paragraphs, Union or Member State law may establish a legitimate ground for processing which has scientific purposes. If this is the case, another exception following from Article 9 might apply to the processing of health data. Since Regulation 536/2014 refers to the applicable law on data protection[927], it should be established whether the basis for the processing of clinical data for scientific purposes remains consent under

922 Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 168.

923 On how this statement can be expressed *see* Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*.

924 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 112. *See* also Koelewijn, "Privacy from a Medical Perspective", pp. 337–338.

925 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 112.

926 The example is provided by Massimiliano Granieri. "Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679". In: *Le Nuove leggi civili commentate* 1 (2017), pp. 165–190.

927 *See* Article 93 of the Regulation 536/2014.

Regulation 536/2014 or if it is a specific Union or Member State law without the consent of the data subject. According to Granieri, this scenario creates possible overlaps of the frameworks and legal uncertainty[928]. In the absence of a specific law, the consent of the subject will be required. Instead, in the presence of law, the rules will constitute the legitimate exception and ground, and they will provide the necessary safeguards and measures that protect the rights of the data subjects.

It is worth noting that consent to processing differs from consent to medical treatment. Both consents shall be informed and free. While the former is related to the specific data processing, the latter represents the free and informed expression of will of the patient who accepts the clinical or medical treatment[929]. The Convention on Human Rights and Biomedicine on the protection of human rights in the biomedical field establishes a general rule on consent by specifying that[930]:

> "An intervention in the health field may only be carried out after the person concerned has given free and informed consent to it. This person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. The person concerned may freely withdraw consent at any time".

Moreover, under the EU Charter of Fundamental Rights in the fields of medicine and biology, the right to the integrity of the person encompasses the respect to free and informed consent of the person concerned[931]. The consent to treatment is a fundamental principle of medical law and it protects the principle of autonomy of the patient[932]. Even though the consent of processing is sometimes not necessary to legitimise the data processing, the healthcare provider shall always obtain consent for the treatment, and then the processing operations can begin.

---

928 *See* Granieri, "Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679".

929 On consent to treatment *see* Herring, *Medical law and ethics*, pp. 155–231.

930 Article 5 of the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (ETS No.164). Oviedo, 04.04.1997. The text is available at <www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98>. Last accessed 06/10/2021.

931 Article 3 of the Charter.

932 Herring, *Medical law and ethics*, p. 155. According to Herring autonomy is the one fundamental ethical principle in the medical arena (p. 207).

Another situation where consent constitutes the legal basis is the processing carried out by commercial entities via mobile-health apps and wearable devices for health- and fitness-related purposes. In these contexts, the "healthcare exception" does not apply since medical professionals are not processing the data and the processing is not carried out under their responsibility, as required by Article 9(3) GDPR[933].

Legitimate grounds are also the obligations and rights in the field of employment and social security and social protection law[934]. The processing of personal health data is lawful when the processing is carried out in an employment, social security and social protection context whether the same processing is necessary for the purposes of carrying out the obligations of, and exercising specific rights of, the controller or of the data subject, and either Union or Member State law or a collective agreement authorises the processing and provides appropriate safeguards for the fundamental rights and the interests of the data subject. In the employment relationship employers normally process personal health data[935]. The main purpose is knowing if the employee is suitable for doing the job offered by the employer[936]. The assessment of working ability is covered by this exception for the employer and the exception of medical diagnosis for the healthcare professional. It has thus been argued that the GDPR made a preventive balance in favour of the employer since this subject can ascertain the work potential of their employee in terms of psycho-physical, attitudinal and technical-professional skills without asking for consent[937]. Another possible purpose is knowing the details of an employee's disability in order to properly adapt the workstation and the safety environment[938]. It seems that the employer has the legitimate interest of processing the employee's data *a priori*. However, the processing is carried out on the basis of Union or Member State law or pursuant to a collective agreement

933 *See* the legal analysis by Mulder, "Health apps, their privacy policies and the GDPR".

934 Article 9(2)(b) GDPR: "(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".

935 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 112.

936 *See* Greco, "Il trattamento dei dati sanitari", p. 229.

937 *See ibid.*

938 *See* Carey, *Data protection: a practical guide to UK and EU law*, p. 71.

that provides appropriate safeguards for the fundamental rights and the interests of the employee. These safeguards should protect the employee from unlawful discrimination during the job. So, the law should minimise the amount of health data to which the employer could have access.

Social security and social protection laws usually refer to occupational medicine which concerns the provision of healthcare assistance to employees and is aimed at preventing any damage caused to health by the conditions of the working environment, such as the risks arising from the presence of harmful objects[939]. The underlying purposes are prevention, diagnosis and therapy activities for the protection of the worker. So, this exception simplifies the processing as indicated for the "healthcare exception".

Furthermore, the individual may be physically or legally incapable of giving explicit consent, especially in healthcare scenarios. The natural person can be unconscious or absent, or he or she may not be reachable[940]. In those circumstances the GDPR then allows processing when it is necessary to protect the vital interests of the data subject or of another natural person[941]. Scholars specified that vital interests are all the existential needs and interests for the protection of life and physical integrity[942]. However, it has been argued that previous wishes of the data subject or the other person are always relevant: if it is known that the individual would not have consented to a processing under the emergency circumstances, the processing cannot be carried out lawfully under this "vital interest exception"[943]. So, an assessment of the data protection interests of the individual is required[944]. This exception instead operates when the processing does not meet the other legitimate grounds and it is necessary to save the life of a person. In the healthcare context, it might be an overlap between this "vital interest exception" and the "healthcare exception". Nevertheless,

939 *See* Greco, "Il trattamento dei dati sanitari", p. 230.

940 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 162.

941 Article 9(2)(c) states that when the "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent", the prohibition does not apply.

942 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 112.

943 *See ibid.*

944 Georgieva and Kuner, "Chapter II Principles (Articles 5–11). Article 9 Processing of special categories of personal data", p. 377.

it has been argued that the former is not limited to the presence of a healthcare professional or a confidential scenario as the latter[945].

Foundations, associations or any non-profit bodies with a political, philosophical, religious or trade union aim can internally process the personal health data of their members, of their former members or of people who have regular contact with them in connection with their purposes when they do not communicate or share the data outside without the consent of the respective data subjects[946]. Some personal health data could be stored by these bodies if necessary for their purposes in light of the data minimisation principle.

Whether the individual makes personal health data public, the processing by a data controller is not prohibited[947]. Nevertheless, the data subject shall deliberately and manifestly make public these data. The publication of personal data shall be a free choice of the individual who makes the data freely available, for example in publicly accessible registers, websites, lists, forums or even public social network profiles[948]. Actually, nowadays there are several forums and websites dedicated to and used by people who suffer from the same disease, such as celiac disease, diabetes, clinical depression, and cancer.

Personal health data are frequently collected and disclosed by subjects for the establishment, exercise or defence of legal claims. This is another legitimate exception. Court cases involving traffic accidents, medical liability, and compensation from insurance companies are daily on the agenda of legal practitioners. Legal claims include court proceedings and administrative or out-of-court procedures[949]. Personal health data shall be related and limited to the specific legal claim for which the subject is

945 *See* Carey, *Data protection: a practical guide to UK and EU law*, p. 73.

946 This exception is provided by Article 9(2)(d): "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects". According to Recital 51 of the GDPR, these entities shall have the purpose of permitting the exercise of fundamental freedoms.

947 Article 9(2)(e) allows the processing that "relates to personal data which are manifestly made public by the data subject".

948 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 113.

949 *Ibid.*

acting. Even the court directly processes personal health data for its ruling, such as when an office technical consultation is arranged. Genetic data are processed in court cases for establishing parentage, or the health status is used as evidence which concerns details of an injury sustained by a victim of crime[950]. When a patient sues the hospital which has provided care, the hospital uses the recorded personal health data as proof in order to defend itself in the course of the legal proceedings[951]. Whenever processing is necessary for these legal claim purposes, the GDPR provides that the general prohibition does not apply[952].

Then, the GDPR establishes some exceptions for reasons of general public interest. In particular, the GDPR seeks to strike a balance between individual interest in the confidentiality of health data and collective interest in the use of these data[953]. So, the processing is lawful for reasons of substantial public interests pursuant to Union or Member State law when it is proportionate to the aim pursued, it respects the essence of the right to data protection and the law provides for suitable and specific measures in order to safeguard the fundamental rights and the interests of the data subjects[954]. Examples of activities carried out by public entities that entail a substantial public interest and that may process personal health data are: keeping public administrative records and registries and certificates of births, deaths and marriages; keeping registries of citizenship, immigration, asylum, and refugee status; carrying out administrative activities and issuance of certifications in connection with healthcare and welfare activities, including organ and tissue transplantation and human blood transfusions; management of public tasks related to occupational safety, population health and safety; granting social protection of motherhood, termination of pregnancy, assistance to the disabled; and providing edu-

950 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 162.

951 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 114.

952 *See* Article 9(2)(f): "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity".

953 *See* Greco, "Il trattamento dei dati sanitari", p. 234.

954 Article 9(2)(g) GDPR. It can be noted that this formulation recalls the "necessity" and "proportionality" tests described in the end of the previous Chapter. Whether a national rule is intended to derogate from the general prohibition, this legislative measure shall pass the two tests and potentially provide safeguards.

cation and training at school[955]. In the e-health sector, some healthcare records may exist, and the data may be processed for substantial public interests on the basis of national statutory law which contains any necessary and proportionate safeguards for a digital processing of personal health data[956].

In addition to general public interest, other Union or Member States regulatory provisions can establish the possibility of processing personal health data for protecting interests in the area of public health[957]. As mentioned, this exception allows the protection of health security, the monitoring and control of diseases or of other serious threats to public health. The law shall define suitable and specific measures to still guarantee the rights and freedoms of individuals, and duties on professional secrecy shall be set. Under the DPD, examples of public health interests were protection against communicable diseases (e.g. HIV) or health promotion (e.g. against cancer and tobacco)[958]. Other examples of public interest in the area of public health are protection against serious cross-border threats to health (e.g. pandemic), and the necessity to ensure high standards of quality and safety of healthcare and of medicinal products or medical devices.

Finally, processing is allowed in accordance with Article 89 of the GDPR for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of proportionate and safeguarding Union or Member State law[959]. Once again, appropriate (i.e.

---

955 This list of examples has been borrowed from the list of processing activities that according to Article 2 *sextes* of the Italian Personal Data Protection Code entails a lawful substantial public interest. Article *sextes* provides the safeguards required by Article 9(2)(g) GDPR. Other examples were adopted before Brexit by the UK Government, which included in the 1998 Act e.g. "carrying on certain types of insurance (relating to disclosure of certain health data of relations of an insured)", "third party data processing for group insurance policies and insurance on the life of another", "identification or prevention of doping in sport". *See* the discussion in Carey, *Data protection: a practical guide to UK and EU law*, p. 76.

956 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 163.

957 Article 9(2)(i) GDPR.

958 *See* Hervey and McHale, *Health law and the European Union*, pp. 330–385.

959 *See* Article 9(2)(j) that allows the processing that is "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law". The law "shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific

necessary and proportionate) safeguards shall be defined for protecting the individuals' rights and freedoms. In particular, technical and organisational measures shall be put in place for ensuring data protection principles, and data minimisation especially[960]. Whether the purposes can be achieved with the use of pseudonymised data, the measure of pseudonymisation shall be implemented. Personal health data may be used for improving scientific research, but specific safeguards should always protect the rights of the data subjects[961].

---

measures to safeguard the fundamental rights and the interests of the data subject". On this basis *see* further Giovanni Comandé. "Ricerca in sanità e data protection un puzzle... risolvibile". In: *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)* 1 (2019), pp. 189–207. On the implementation of Article 89 in Member States' legislation *see* TIPIK, *Report on the implementation of specific provisions of Regulation (EU) 2016/679*, pp. 29–39; DG Health and Food Security. *Assessment of the EU Member States' rules on health data in the light of the GDPR*, pp. 60–81.

960 Article 89(1) GDPR. The following paragraphs of this provision provide the possibility for Union or Member State law to derogate from data subjects' rights by stating that: "2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs".

961 On how the GDPR affected clinical research *see* the interesting study by Jacques Demotes-Mainard et al. "How the new European data protection regulation affects clinical research and recommendations?" In: *Therapie* 74.1 (2019), pp. 31–42. As mentioned in the first Chapter the interactions between Big Data and e-health data are beyond the scope of this book. However, for a synthesis on the possible uses and concerns of data analytics for healthcare *see* Menno Mostert et al. "From privacy to data protection in the EU: implications for big data health research". In: *European Journal of Health Law* 25.1 (2017), pp. 43–55, which provides the EU regulatory perspective; MIT Critical Data and M. Komorowski. *Secondary analysis of electronic health records*. Springer, 2016. ISBN: 9783319437422, which provides the technical perspective; I. Glenn Cohen and Harry S. Graver. "Cops, docs, and code: a dialogue between big data in health care and predictive

Regulation 2018/1725 is aligned with the GDPR, So, it provides similar legitimate grounds for the processing of sensitive data, but when referring to safeguards and other rules it mentions Union law only[962]. As regards a final comparison with the previous legal framework, the legal grounds for the processing of personal health data according to the GDPR and the Data Protection Directive are similar[963]. The GDPR uses several exceptions of the DPD and mainly adds the possibility of derogating from the prohibition for public interest in public health and archiving, research and statistics purposes[964]. In the exception related to the employment field, the GDPR also specifies social security and social protection law, which were never provided. The comparison of the legitimate exceptions is further described in the detailed Table 3.1.

Table 3.1 Synthesis of the comparison between GDPR and DPD

LEGITIMATE BASIS	GDPR	DPD
Explicit consent	Art. 9(2)(a)	Art. 8(2)(a), without the possibility of derogation
Obligation and rights in the field of employment, social security, social protection law	Art. 9(2)(b)	Art. 8(2)(b), but only employment law
Vital interest	Art. 9(2)(c)	Art. 8(2)(c)

policing". In: *UCDL Rev.* 51 (2017), p. 437, which provides the US regulatory perspective. For a general commentary on healthcare scientific research and GDPR *see* Giulia Schneider. "Disentangling health data networks: a critical analysis of Articles 9 (2) and 89 GDPR". in: *International Data Privacy Law* (2019), pp. 253–271; Denise Amram. "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks". In: *Computer Law & Security Review* 37 (2020), p. 105413; Rossana Ducato. "Data protection, scientific research, and the role of information". In: *Computer Law & Security Review* 37 (2020), p. 105412.

962 *See* Article 10 Regulation 2018/1725.

963 For other comparisons with the DPD *see* Pormeister, "The GDPR and Big Data: Leading the Way for Big Genetic Data?", p. 7 and Georgieva and Kuner, "Chapter II Principles (Articles 5–11). Article 9 Processing of special categories of personal data", pp. 375–376.

964 With reference to a comparison *see* e.g. Greco, "Il trattamento dei dati sanitari".

LEGITIMATE BASIS	GDPR	DPD
Data processed by non-profit entities	Art. 9(2)(d)	Art. 8(d), but limited
Data made public	Art. 9(2)(e)	Art. 8(2)(e)
Legal claim use	Art. 9(2)(f)	Art. 8(2)(3), but not the courts in the judicial capacity
Substantial public interest	Art. 9(2)(g)	Art. 8(2)(a)
Preventive or occupational medicine, assessment of the working capacity, medical diagnosis, medical treatment, management of health ser- vices and systems subject to conditions provided by law	Art. 9(2)(h)	Art. 8(3), but not occupational medicine, assessment of the working capacity, or social care system
Execution of a contract with healthcare professional	Art. 9(2)(h)	Not explicitly provided
Public interest in public health	Art. 9(2)(i)	Not provided, but Art. 8(4) referred to substantial public interest generally
Archiving in public interest, scientific, historical research, statistic	Art. 9(2)(j)	Not provided

Moreover, the legal grounds for the processing of health data according to the GDPR and to the CoE's Recommendation CM/Rec (2019) 2 are essentially the same, as shown by Table 3.2[965]. After a comparison of the rules, it can be argued that where it is not further explained the lawful grounds coincide.

965 *See* Article 5 of the Recommendation CM/Rec (2019) 2.

Table 3.2 Synthesis of the comparison between GDPR and CoE's Rec.

LEGITIMATE BASIS	GDPR	RECOMMENDATION
Explicit consent	Art. 9(2)(a)	Art. 5(b)
Obligation in the field of employment, social security, social protection law	Art. 9(2)(b)	Art. 5(a) employment and social protection
Vital interest	Art. 9(2)(c)	Art. 5(a)
Data processed by non-profit entities	Art. 9(2)(d)	Not provided
Data made public	Art. 9(2)(e)	Art. 5(d)
Legal claim use	Art. 9(2)(f)	Art. 5(a), not specifying the courts but also "reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services, subject to the conditions provided for by law"
Substantial public interest	Art. 9(2)(g)	Art. 5(a)
Preventive or occupational medicine, assessment of the working capacity, medical diagnosis, medical treatment, management of health ser- vices and systems subject to conditions provided by law	Art. 9(2)(h)	Art. 5(a), but not occupational medicine or assessment of the working capacity
Execution of a contract with healthcare professional	Art. 9(2)(h)	Art. 5(c)

LEGITIMATE BASIS	GDPR	RECOMMENDATION
Public interest in public health	Art. 9(2)(i)	Art. 5(a), such as the protection against health hazards, humanitarian action or high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions provided for by law
Archiving in public interest, scientific, historical research, statistic	Art. 9(2)(j)	Art. 5(a), but further conditions in Chapter V

Thus, at the EU level the legitimate grounds for processing of personal health data are overall consistent. Member State or Union law will provide the appropriate safeguard where derogation is set and they may establish further rules, but the main requirements are still laid down by the GDPR. So far, the notions and the exception which allow the processing of personal health data have been examined. The next section deals with the other data protection rules the data controller shall comply with in the context of e-health.

3.3.3 The relevant and applicable provisions of the GDPR

This section now summarises the other provisions of the GDPR that are relevant for the processing of personal health data. As much as in other fields, the application of the GDPR radically changed the protection of data by increasing the rights to be protected and the obligations to comply with[966]. In fact, in the context of personal health data some clarifications on the exercise of data subjects' rights and duties of the controller are indispensable. It is worth stressing that the concrete application of the

966 On the changes for the healthcare context after the GDPR *see* e.g. the Italian book Giuseppe Carro, Sarah Masato, and Massimiliano Domenico Parla. *La privacy nella sanità*. Giuffrè, Torino, 2018. ISBN: 9788814225215.

GDPR depends on a case-by-case basis, and the e-health technology being used. Nevertheless, the interpreter can make some general opinions on data protection in this specific field.

First of all, the patient has the right to be informed on the processing in the e-health technology in a separate way than the information received on the treatment (e.g. when seeking consent to the treatment). Whether the processing is based on the explicit consent of the data subject (e.g. the well-being app), the information on the existence of the right to withdraw this consent at any time shall be provided to the individual by specifying that his or her choice does not affect the lawfulness of processing based on prior consent[967].

Under the GDPR, the data subject has the right to receive more information than under the DPD, such as the contact details of the DPO, the data storage period or the criteria used to determine it, the existence of the right to lodge a complaint to a supervisory authority and of automated decision-making or profiling. So, the privacy policies shall be updated, and adequate in accordance with this new framework[968].

Generally, the right to access is highly important in the e-health field. According to Recital 63 of the GDPR data subjects have the right to access their personal health data in their medical records which contain different information such as "diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided"[969]. This right may be exercised by electronic means. It has been claimed that the condition established by the GDPR for the right to access – which should not negatively affect the "rights or freedoms of others, including trade secrets or intellectual property" – might limit the right in the healthcare context[970]. However, this limitation might only apply in the cases where algorithms are used for generating the data, and the data controller may want to protect its IP rights. In the traditional e-health context, the patient has the right to access personal general and health data. The right to access implies also the right to obtain information on processing, such as important information on the recipients, and the right to obtain a copy

967 *See* Article 13(2)(c) and Article 14(2)(d) GDPR.

968 The importance of the use of user-friendly documents (e.g. icons), and the need to use an adequate, plain and clear language have been already highlighted in the previous Chapter, Section 2.4.8.

969 Recital 63 GDPR. *See* also Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 151.

970 *See* Malgieri and Comandé, "Sensitive-by-distance: quasi-health data in the algorithmic era".

of the data being processed, that in the e-heath context may be provided in electronic form[971]. It is even possible for patients to request from the healthcare provider the log files to see who has accessed their data (e.g. medical staff)[972].

The right to rectification in the e-health field is particularly valuable since personal health data are often processed for medical diagnosis, assessment of the working capacity, or provision of social care. As mentioned, the accuracy and quality of data are essential for guaranteeing effective and efficient healthcare provision. Data subjects can easily ask for the rectification of common personal data by providing accurate data directly to the controller. However, patients may not be able to provide the accurate personal health data that should be processed in the e-health technology. Data subjects may instead ask the controller to rectify data which does not correspond to reality as far as they are aware. The controller will check the information, and if needed rectify inaccurate data[973].

The right to erasure is not easily applicable in the e-health context[974]. Whenever the data controller has a legal obligation to store and keep the data in accordance with a Union or Member State law (e.g. clinical information systems), or the subject is performing a task in the public interest or in the exercise of official authority (e.g. disease registries and systems for healthcare management), the data will not be erased in accordance with Article 17 GDPR[975]. Indeed, in the healthcare context the registries of the treatments are kept in accordance with the law not only for monitoring the patient, but also for proving the healthcare service performed by the professional. Public hospitals or healthcare entities are usually public administrations, which are not subject to the obligation of data erasure upon request. Moreover, Union or Member State law may prevent the erasure of data in the area of public health to protect the public interest involved, or for archiving, scientific, research, statistic or historical purposes, and the same law may potentially establish the appropriate safeguards (e.g. pseudonymisation)[976]. It has even been argued that the exceptions of

971 *See* Article 15 GDPR.
972 *See* Guarda, "I dati sanitari", p. 611.
973 *See* Article 16 GDPR.
974 As indicated in Chapter 2 Section 2.4.8, the right to erasure is established in Article 17.
975 Article 17(3)(b) GDPR.
976 Article 17(c) GDPR states that the right to erasure or to be forgotten does not apply if processing is necessary "for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Arti-

Article 17, which prevents erasure upon request by the data subject, imply not only protection against cross-border threats to health, and the need to ensure high standards of quality and safety of healthcare, medical products and devices, but also all the grounds of the "healthcare exception" of Article 9[977]. So, the data subjects of this processing may never obtain the erasure of data unless the timing of storage and the activities are lawfully finished. Another exception to the right to erasure is the need to keep data for the exercise or defence of legal claims, which here are usually related to medical malpractice, breach of confidentiality, or failure by healthcare providers to perform their duties[978].

Therefore, the right to be forgotten in the sense of the GDPR may apply in a few residual cases, such as the use of e-health apps. As indicated in the previous section, it is possible that the data subject has given the consent to processing with a purpose other than medical treatment (e.g. consent to clinical trial, or to an app) – this consent is the legal ground of the processing – but he or she decides to withdraw it. Whether no other ground applies, the data subject has the right to obtain the erasure of their data in accordance with Article 17(1)(b) GDPR. Another case where the erasure applies is the unlawful processing of personal health data[979]. If the controller has carried out the processing without a lawful legal ground, the data subject has the right to obtain erasure from the data controller.

Some Member States established a different right of concealment of specific personal health data[980]. In this case, data is not erased, but it is not intelligible to users of the e-health system without specific and exceptional permission. However, it can be argued that it is in the interest of the patient that the personal data are not erased in order to receive accurate and efficient care in the future. It might be the case that the patient asks for the erasure of common personal data, such as administrative data,

---

cle 9(3)". Moreover, Article 17(d) GDPR specifies that "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing", the data subject does not have the right to obtain erasure.

977 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 160. Therefore, the exception may cover the grounds of Article 9(2)(h) and (i) GDPR.

978 Article 17(1)(e) GDPR.

979 Article 17(1)(d) GDPR.

980 For example, this right has been specified by the Italian and French legal frameworks for the EHR. *See* further for sources and explanation in Section 3.4.2.

address, or e-mail. The data controller shall determine whether these data are necessary for the main purpose. If so, the data will not be erased. If not, the controller will evaluate the exceptions mentioned above following a case-by-case approach.

Special considerations on the right to restriction for the processing of personal health data do not seem necessary. The controller can assess whether the four conditions of Article 18 GDPR apply. So, whether the data subject has contested the accuracy of the data, or the processing is unlawful, he or she may have the right to obtain a restriction. The same right may apply where the purposes of the processing are satisfied, but the data subject may need the data for the establishment, exercise or defence of legal claims, or where a request of objection is pending[981]. However, the right to object does not seem applicable in the e-health context as the provision of Article 21 refers to processing based on two grounds of Article 6, meaning the public task of an authority or the legitimate interest of the controller or a third party, and to marketing purposes. The common personal data processed in an e-health scenario are usually necessary or accessory for the processing of personal health data. Thus, the right to object might never apply in this field[982].

As regards the right to portability of Article 20 GDPR, it has been argued that it applies only insofar as the patient has provided their personal health data to the healthcare provider in a medical file or personalised health environment[983]. So, the portability can concern health data collected through the monitoring and recording of the subject's activities, such as heartbeat data recorded in a mobile health app[984]. However, the right to portability applies to data provided by the data subject and observed in the system, but it does not apply to inferred data and complex data which are generated by the controller[985]. It should be noted that whether the controller performs the healthcare task in the public interest or in the exercise of an official authority, the right to portability shall not apply. Therefore, once again, public hospitals may not apply this right. Nevertheless, the exercise and application of this right may foster access

981 *See* Article 18(1)(a) – (d) GDPR.
982 *See* Article 21(1) GDPR.
983 *See* Hooghiemstra, "Informational Self-Determination, Digital Health and New Features of Data Protection", p. 169.
984 Guarda, "I dati sanitari", p. 612.
985 *See* Malgieri and Comandé, "Sensitive-by-distance: quasi-health data in the algorithmic era", p. 247; Lynskey, "Chapter III Rights of the Data Subject (Articles 12–23). Article 20. Right to data portability", p. 503.

to healthcare in territories other than the one where the patient is treated, and cross-border access to healthcare, too[986]. The right to portability is also recommended by CoE Recommendation CM/REC (2019) 2, which stresses the importance of data transmission from one controller to another[987]. Indeed, portability may enhance continuity of care of a patient.

Moreover, profiling and automated decision-making are increasingly used in the healthcare context[988]. Under the GDPR the definition of profiling includes health as an aspect which is analysed or predicted by automated activities[989]. The health status can be inferred from raw data[990]. The application of Article 22 in the e-health context may be related to the use of AI for analysing aspects of a data subject's health or of the diagnosis[991]. The right to not be subject to automated processing applies almost always in the case of personal health data since they are sensitive data[992]. Nevertheless, Article 22(4) explicitly establishes that the right to not be subject to a decision based solely on automated processing is not applicable whether the data subject has given the explicit consent or the processing is necessary for reasons of a substantial public interest, and suitable safeguards are put in place[993]. The adopted safeguards and measures

986 A specific section of this book is dedicated to cross-border healthcare. *See infra* 3.4.3.

987 The right to portability is even recommended by Recommendation CM/REC (2019) 2 at Article 12.5, which specifies: "where the processing is performed by automatic means, the data subject should be able to obtain from the controller, subject to conditions prescribed by law the transmission – in a structured, interoperable and machine-readable format – of their personal data with a view to transmitting them to another controller (data portability). The data subject should also be able to require the controller to transmit the data directly to another controller".

988 *See* Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.

989 *See* Article 4 (4) and Recital 71 GDPR.

990 As explained *infra* in Section 3.3.1, personal health data may be derived from common personal data which are combined through algorithms.

991 *See* Dimitra Kamarinou, Christopher Millard, and Jatinder Singh. "Machine Learning with Personal Data: Profiling, Decisions and the EU General Data Protection Regulation". In: *Journal of Machine Learning Research* (2017); Pierce, "Machine learning for diagnosis and treatment: Gymnastics for the GDPR".

992 *See* Gianclaudio Malgieri and Giovanni Comandé. "Why a right to legibility of automated decision-making exists in the general data protection regulation". In: *International Data Privacy Law* (2017), p. 246.

993 Article 9(4) states: "Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or

shall correspond to the high sensitivity of data[994]. So, in these cases the data subjects have the right to obtain human intervention, express their individual point of view, and contest the automatic decision[995].

Finally, Union or Member State law may restrict the rights outlined above in accordance with Article 23 GDPR to protect other interests. As discussed above, the health sector is frequently subject to other national rules that derogate from or further specify the processing activities only insofar as the legislative measure is necessary and proportionate, and it respects the rights and freedoms of individuals in a democratic society. In sum, the considerations on the rights are indicated in the following Table 3.3.

Table 3.3 Data subject's rights as a patient

RIGHT	APPLICATION IN E-HEALTH FIELD
Right to be informed	Obtaining information on processing in a separate form than information on the treatment
Right to access	Having access to medical records and obtaining related information and a copy of data
Right to rectification	Obtaining rectification of inaccurate or incomplete health data in the system
Right to erasure	Several exceptions from the application
Right to restriction	Obtaining temporary restriction of processing

(g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place".

994 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 183.

995 *See* Malgieri and Comandé, "Why a right to legibility of automated decision-making exists in the general data protection regulation", p. 246. According to the authors the right to explanation is not legally binding since it is specified in Recital 71 only.

RIGHT	APPLICATION IN E-HEALTH FIELD
Right to data portability	Receive personal health data provided by the subject and having them ported to another con- troller under certain circumstances
Right to object	Not easily applicable
Right to human intervention	Exceptions from the application in case of explicit consent and substantial public interest, and safeguards apply

In the accountability-based approach of the GDPR, some organisational requirements are established for processing sensitive data because this processing is "very risk-prone"[996]. Whether personal health data are processed on a large scale, the data controller shall[997]:
- maintain the record of processing;
- notify or communicate a data breach;
- carry out a DPIA;
- designate a DPO;
- implement appropriate technical and organisational measures based on the high risk potential.

In Chapter 2, Section 2.4.5, it has been claimed that the expression "on a large scale" is broad and open to interpretation[998]. It can be argued that processing is on a large scale when it involves considerable amounts of

996 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 116.

997 Even the CNIL listed the measures required in the healthcare context. The authority identified the measures as follows: "mettre en place un registre des traitements; mener des analyses d'impact pour les traitements considérés comme présentant un risque élevé pour les personnes; veiller à encadrer l'information des personnes concernées (patients, fournisseurs, étudiants, usagers, etc.) et s'assurer de l'effectivité de leurs droits (droit d'accès, de rectification, d'opposition, etc.); formaliser les rôles et responsabilités du responsable de traitement; lorsque cela est obligatoire, désigner un délégué à la protection des données (DPO); renseigner les actions menées pour garantir la sécurité des données". *See* the comment at <www.cnil.fr/fr/ quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel>. Last accessed 06/10/2021.

998 On the same opinion *see* Granieri, "Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679".

data at a regional, national or supranational level or when it potentially affects a large number of data subjects[999]. Article 29 Working Party defined some criteria to determine whether the processing is on a large scale, namely the number of data subjects, the volume of data and/or the range of different data items, the duration, or permanence, of the data processing activities, and the geographical extent of these activities[1000]. According to Article 30 GDPR, the data controller and processor who process sensitive data shall maintain a record of processing activities[1001]. The provision lists the information that the records should contain. For the e-health context, where the risk is high, describing the technical and organisational security measures is essential.

A data breach in the e-health context is likely to result in a high risk to the rights and freedoms of the data subjects[1002]. Therefore, the data controller shall notify the DPA of the personal data breach without undue delay, and if feasible no later than 72 hours after being made aware, by communicating details of the breach[1003]. At the same time, the personal data breach shall be communicated to the data subjects without undue delay unless the conditions indicated in Article 34(3) are met (e.g. the implementation of appropriate measures)[1004]. Typical and frequent examples of data breach in the e-health context are: sending the laboratory result to a person other than the recipient indicated in the instructions given to the patient, the publication of personal health data in open websites or forums, and the use of a personal pen-drive by the medical professional who then lost it[1005].

The designation of the data protection officer is binding for the processing of health data on a large scale and when this processing is a core activity of the controller or processor[1006]. Public administration shall designate a DPO, too[1007]. Therefore, hospitals, private clinics, and private

999 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 48.
1000 *See* Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 10.
1001 Article 30(5) GDPR.
1002 *See* Guarda, "I dati sanitari", p. 611.
1003 *See* Article 33 GDPR.
1004 *See* Article 34 GDPR.
1005 *See* Carro, Masato, and Parla, *La privacy nella sanità*, pp. 77–78.
1006 Article 37(1)(c) GDPR.
1007 Article 37(1)(a) GDPR.

healthcare providers shall choose an independent DPO[1008]. Among the core activities of the hospital is the processing of health data since the provision of healthcare implies the collection the recording of health information[1009]. In addition to these cases, the processing of health data via wearable devices can be included in the notion of "regular and systematic monitoring" of Article 37(1)(b) GDPR[1010]. Therefore, the mandatory designation applies. There might be a single DPO for several healthcare facilities, unless they are hard to reach by the officer who has to efficiently and promptly support each data controller[1011].

Under the DPD, Member States required notification to the DPA of processing involving sensitive data[1012]. Under the GDPR, this notification is not required yet. However, the data controller that processes personal health data on a large scale shall carry out a DPIA in accordance with Article 35. The high risk in processing health data is *in re ipsa*[1013]. A DPIA is not mandatory for an individual physician or a healthcare professional, independently of the amount of data processed[1014]. A DPIA is instead mandatory for a hospital which processes patients' personal data in the hospital information system, since data are sensitive and processed on a large scale[1015]. The processing of personal health data in research projects and clinical trials is likely to require a DPIA as well, since they store a great amount of sensitive data[1016]. Actually, it has been pointed out that

1008 Guarda, "I dati sanitari", p. 611. On the role of the DPO in processing of personal health data *see* also Giorgio Pedrazzi. "Il ruolo del Responsabile della protezione dei dati (DPO) nel settore sanitario". In: *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)* 1 (2019), pp. 181–186.

1009 Hospitals are examples in the investigation of core activities in Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, p. 20.

1010 *See* Article 29 Working Party, *op. cit.*, p. 21.

1011 *See* Carro, Masato, and Parla, *La privacy nella sanità*, that recalls the WP opinion on DPO.

1012 *See* Article 18 of the DPD.

1013 Granieri, "Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679". *See* also Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 9.

1014 *See* Recital 91 GDPR and Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 51.

1015 This is an example where the DPIA is likely to be required by WP29. *See* Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 11.

1016 *See ibid.*

the majority of medium-to-large healthcare facilities shall assess the risk through the DPIA, and even smaller ones, whether or not they have an agreement with the public national health service and are compared to this public entity[1017].

Moreover, Article 36 requires prior consultation of the controller with the DPA when the DPIA indicates that the processing has high risk, and the envisaged measures cannot mitigate this risk[1018]. Member States' law may establish a binding prior consultation for the processing carried out for reasons of public interest in the area of public health[1019].

Healthcare providers shall comply with the DPbD and DPbDf obligations, and the security principle. According to Article 83(2)(g) GDPR, the DPA will take into account the category of personal data subject to the violation. Indeed, the appropriate technical and organisational measures necessary to ensure the implementation of data protection principles apply even more for the special categories of data[1020]. The application of DPbD in the context of e-health implies the appropriate design of the technologies and services which process personal health data. E-health technologies shall be privacy- and data protection- compliant from the development stage[1021]. DPbD (and PbD) may reassign to the patient a crucial role within the care process, at the centre of the data flow[1022]. It has been argued that regulation by design for healthcare can facilitate the design of new health management infrastructure and helps achieve a good balance between care needs, individual protection of patients' fundamental rights and public health interests[1023]. DPbD is fundamental in the context of e-health, which requires an interdisciplinary approach "by default" and a

1017 *See* Carro, Masato, and Parla, *La privacy nella sanità*, p. 28.
1018 Article 36(1) GDPR.
1019 Article 36(5) GDPR. *See* also Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 19.
1020 Durst, "Il trattamento di categorie particolari di dati in ambito sanitario", p. 67.
1021 *See* Melchionna and Cecamore, "Le nuove frontiere della sanità e della ricerca scientifica", p. 598.
1022 Raffaella Brighi and Maria Gabriella Virone. "Una tutela 'by design' del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica". In: *A Matter Of Design. Making Society Through Science And Technology* (2014), pp. 1211–1222, p. 1218.
1023 *Ibid.*

correct implementation of the principles from the beginning of the design stage[1024].

As the DPbD requires a case-by-case approach, a case study will be presented in the e-health domain. The selected technology is an Electronic Health Record system and it is further analysed in the next sections.

3.4 The case study of Electronic Health Record system

EU policies on health and care stress the importance of the use and implementation of e-health systems, such as EHRs, since they allow more targeted, personalised, effective and efficient healthcare and reduce errors and length of hospitalisation[1025]. Electronic Health Record is a solution that can substitute the established, paper-based, health service[1026]. In this book this case study has been selected since it refers to a widely used technology which is considered a priority by EU policies and strategies. Actually, it is a key element for e-health policies at the EU level and is at

1024 *See* Guarda, "I dati sanitari", p. 609; Faralli, Brighi, Martoni, et al., *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health*, p. 304.

1025 *See* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union".

1026 In the classification of the Expert Panel on effective ways of investing in Health, *Assessing the impact of digital transformation of health services*, EHR is an example of substituting an established health service. In general, on EHR *see* Paolo Guarda. *Fascicolo sanitario elettronico e protezione dei dati personali*. Vol. 94. Università degli Studi di Trento, Quaderni del Dipartimento di Scienze Giuridiche, 2011. ISBN: 9788884433671; Carolyn P. Hartley and Edward Douglass Jones. *EHR implementation: A step-by-step guide for the medical practice*. American Medical Association, 2012. ISBN: 9781603596305; Giovanni Comandé, Luca Nocco, and Violette Peigné. "Il fascicolo sanitario elettronico: uno studio interdisciplinare". In: *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)* 1 (2012), pp. 106–121; Nicholas P. Terry and Leslie P. Francis. "Ensuring the privacy and confidentiality of electronic health records". In: *U. Ill. L. Rev.* (2007), pp. 681–736; Eric J. Bieber, Frank M. Richards, and James M. Walker. *Implementing an electronic health record system*. Springer, 2005. ISBN: 9781846281150; Carlisle George, Diane Whitehouse, and Penny Duquenoy. *eHealth: legal, ethical and governance challenges*. Springer Science & Business Media, 2012. ISBN: 9783642224744.

the heart of e-health practices[1027]. EHR represents a pivotal moment in the digitalisation of health data processing[1028].

The EHR aims to empower the patient, who becomes a crucial point in the information management system[1029]. This processing helps healthcare providers to better manage patients' treatment with accurate, up-to-date and complete data by enabling quick access to a digital record, which embeds diagnoses and prescriptions[1030]. As reported for the opportunities of e-health technologies, the EHR can reduce medical errors, allows a more effective treatment, and supports physicians' decision making[1031].

This technology is regularly used for the processing of personal health data in hospitals or clinics by general practitioners or specialist professionals[1032]. The EHR is an important digital tool for healthcare providers and hospitals since it archives all the personal health data of the patient and shares them among all the authorised operators who are entitled to the health treatment[1033]. For the sake of completeness, it is necessary to specify that in the literature the term Personal Health Record (PHR) is frequently used to indicate a digital record managed and controlled by the patient[1034]. This investigation mainly focuses on the EHR system, where

---

1027 *See* Arak and Wójcik, *Transforming eHealth into a political and economic advantage*, p. 14; Placide Poba-Nzaou and Sylvestre Uwizeyemungu. "Variation in electronic health record adoption in European public hospitals: a configurational analysis of key functionalities". In: *Health and Technology* 9.4 (2019), pp. 439–448, p. 440.

1028 *See* Paolo Guarda. "Biobanks and electronic health records: open issues". In: *Comparative Issues in the Governance of Research Biobanks*. Springer, 2013, pp. 131–141. ISBN: 9783642331169, p. 133.

1029 *Ibid.*

1030 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 162.

1031 Ilias Iakovidis. "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe". In: *International journal of medical informatics* 52.1 – 3 (1998), pp. 105–115, p. 107. *See* also on the significance of the EHR Pradeep K. Sinha et al. *Electronic health record: standards, coding systems, frameworks, and infrastructures*. Wiley – IEEE Press, 2013. ISBN: 9781118281345, pp. 6–7.

1032 *See* the analysis on EU public hospitals in Poba-Nzaou and Uwizeyemungu, "Variation in electronic health record adoption in European public hospitals: a configurational analysis of key functionalities".

1033 Guarda, "I dati sanitari", p. 616.

1034 *See* e.g. Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*; Yakov Flaumenhaft and Ofir Ben-Assuli. "Personal health records, global policy and regulation review". In: *Health policy* 122.8 (2018), pp. 815–826. The PHR could be synchronised with the EHR on patient re-

the contribution of the patient to the system is potentially available, but is not the primary source in terms of personal data, such as in the PHR system[1035].

In the past, all patients' information was collected on paper records, whereas in the e-health context it is often digitalised in an EHR system[1036]. The EHR goes beyond the paper-based record[1037]. Some authors defined this technology as the most important, and perhaps the most challenging, of the technological developments in the e-health context since it links and adds value to the other technologies[1038]. The EHR allows the data exchange between patients, healthcare providers, clinicians and pharmacies in order to support both individuals and physicians in accessing and providing care[1039]. EHR is designed to record and make accessible all data that are useful for the healthcare treatment[1040]. It is more than a tool because it is a complex system with several capabilities and functions[1041].

---

quest. *See* Rishi Saripalle, Christopher Runyan, and Mitchell Russell. "Using HL7 FHIR to achieve interoperability in patient health record". In: *Journal of biomedical informatics* 94 (2019), p. 103188. PHR is only one of the multiple models of digital repositories for healthcare. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 29–31, reportes that other systems are Electronic Medical Record (EMR) and Electronic Patient Record. On PHR *see* also Guarda and Ducato, "From electronic health records to personal health records: emerging legal issues in the Italian regulation of e-health"; Kim Wuyts et al. "What electronic health records don't know just yet. A privacy analysis for patient communities and health records interaction". In: *Health and Technology* 2.3 (2012), pp. 159–183, pp. 162–166.

1035 On the differences between the two tools *see* also Giovanni Comandé, Luca Nocco, and Violette Peigné. "An empirical study of healthcare providers and patients' perceptions of electronic health records". In: *Computers in Biology and Medicine* 59 (2015), pp. 194–201, p. 194.

1036 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 162.

1037 The reason will be further explained in Section 3.4.1, where a brief comparison will be provided. On the main differences *see* e.g. G Hayes. "The requirements of an electronic medical record to suit all clinical disciplines". In: *Yearbook of medical informatics* 6.01 (1997), pp. 75–82.

1038 *See* Katsh and Rabinovich-Einy, "The Internet of On-Demand Healthcare", p. 89.

1039 *See* OECD, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*.

1040 *See* Wicks, "Electronic health records and privacy interests: The English experience", p. 75.

1041 *See* Katsh and Rabinovich-Einy, "The Internet of On-Demand Healthcare", p. 91; Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*.

Therefore, EHRs provide the opportunity to access to personal health data ubiquitously, as the entire patient's medical history is potentially available online[1042].

In general terms, at its core an EHR is a system that healthcare providers use for documenting, monitoring, and managing healthcare delivery within their organisations[1043]. So, an EHR system seems clinician-focused, and the data processing seems limited to a single healthcare entity of the National Health Service (NHS). However, multiple providers may have access to the system, such as the general healthcare practitioner, pharmacists, professionals in a hospital or clinic, and other healthcare professionals of a Member State[1044]. Indeed, EHRs may contain information from all health care providers involved in the patient's care[1045]. Even a cross-border healthcare provision, and data processing, may be carried out in accordance with the EU interoperability policies on EHRs.

For these reasons, EHR systems raise data protection concerns that did not exist in the paper-based scenario. In the next sections, the investigation on this e-health solution deals with the state of the art of this technology, the issues of the applicable legal framework at the EU level, and the policies that enable cross-border processing within the problems that this processing entails.

3.4.1 The state of the art of EHR

The aim of this section is to briefly define the common core of data in an EHR and the common features and properties of this e-health technology. In general, the literature commonly defines an EHR as "a standard-based machine-processable information entity consisting of health data pertaining to an individual and resulting in an exhaustive aggregation of personal health data, which is longitudinal, cross-institutional and multi-

1042 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 162.

1043 *See* Aceto, Persico, and Pescapé, "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges", p. 132.

1044 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 338, which includes EHRs in the notion of e-health and mentions multiple actors.

1045 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 162.

modal"[1046]. From the technical point of view, the personal health data in the EHR are collected by several entities as source systems (i.e. healthcare providers), which aggregate data in repositories in a given period of time (e.g. patient's life period), and use the whole resulting system of different ways of interaction. The EHR system consists in different connected elements. EHR then enables the provision of healthcare across organisations[1047]. It potentially streamlines the clinician's workflow[1048].

It has been pointed out that defining what is an EHR is very complex[1049]. The notion is an evolving concept[1050]. The ISO definitions related to EHR and Health Informatics have been framed after many attempts and several drafts since encapsulating the existing differences in the state of the art is not simple[1051]. Following ISO standard 20514:2005(en) on EHR, the useful definitions related to this technology can be textually reported in the following Table 3.4[1052]. ISO's definitions differentiate between EHR for integrated care and generic EHR because "there are still currently many variants of the EHR in health information systems which do not comply with the main EHR definition". Therefore, for the purpose of the present book the term EHR is identified by the generic ISO's definition outlined in the Table.

1046 Amnon Shabo. "Electronic Health Record". In: *Encyclopedia of Database Systems*. Springer, 2017, pp. 101–177. ISBN: 9781489979933.

1047 *See* Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*, p. 4.

1048 Quintana and Safran, "Global health informatics — an overview", p. 4.

1049 *See* e.g. Shabo, "Electronic Health Record"; Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*.

1050 Wuyts et al., "What electronic health records don't know just yet. A privacy analysis for patient communities and health records interaction".

1051 *See* Shabo, "Electronic Health Record", which summarises attempts to define EHR by commenting on the draft of ISO/TC 215 technical report. Electronic health record definition, scope, and context. Second draft of August 2003.

1052 The definitions are listed in the second Chapter of the standard in ISO. *Health informatics — Electronic health record — Definition, scope and context. 20514:2005(en)*. Tech. rep. ISO/TR, 2005.

Table 3.4 Definitions of ISO/TR 20514:2005

OBJECT	DEFINITION
Electronic Health Record for Integrated Care (ICEHR)	"Repository of information regarding the health status of a subject of care, in computer processable form, stored and transmitted securely and accessible by multiple authorised users, having a standardised or commonly agreed logical information model that is independent of EHR systems and whose primary purpose is the support of continuing, efficient and quality integrated health care"
Electronic Health Record (EHR)	"Repository of information regarding the health status of a subject of care, in computer processable form"
Electronic Health Record Architecture (EHRA)	"Generic structural components from which all EHRs are built, defined in terms of an information model"
EHR extract	"Unit of communication of all or part of the EHR which is itself attestable and which consists of one or more EHR compositions"
EHR node	"Physical location where EHRs are stored and maintained"
EHR system	"Set of components that form the mechanism by which electronic health records are created, used, stored and retrieved including people, data, rules and procedures, processing and storage devices, and communication and support facilities"
Functional interoperability	"Ability of two or more systems to exchange information"

OBJECT	DEFINITION
Semantic interoperability	"Ability for information shared by systems to be understood at the level of formally defined domain concepts"

So, while the EHR is a record – a data repository related to the health status of the data subject in electronically maintained form – the EHR system is a more complex concept, which includes several components that form the mechanism by which the EHR is used. In particular, it entails both an organisational level with "people, data, rules and procedures" and a technical level with "processing and storage devices, and communication and support facilities".

Moreover, the notions of functional and semantic interoperability are essential in this environment since the different sources of the record must be able to share and exchange information. Generally, interoperability means "the ability of a system or a product to work with other systems or products without special effort on the part of the customer"[1053]. Interoperability means not only that "information can be exchanged between many systems or services", but that "the receiving system is able to use the information to perform new actions"[1054]. The notion consists of many layers, namely technical, semantic, organisational and legal interoperability[1055]. Given two different systems, A and B, technical interoperability allows the exchange of data from A to B by neutralising the distance, while semantic interoperability ensures that A and B understand the data in the same way without ambiguity[1056]. It has been pointed out that, on the one hand, at a semantic level the formats by which the EHR is created should be reconciled; on the other hand, at a technical level the challenge is finding

1053 Standards University IEEE. *Standards Glossary*. IEEE, 2016.

1054 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 2, which reports the definitions in Arak and Wójcik, *Transforming eHealth into a political and economic advantage*.

1055 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3.

1056 *See* A. Soceanu. "Managing the Interoperability and Privacy of e-Health Systems as an Interdisciplinary Challenge". In: *Systemics, Cybernetics and Informatics* 14.5 (2016), pp. 42–47; Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3.

the appropriate approach for aggregating the data[1057]. Since "integration" is a core functionality of the EHR, the integration effort has always been a challenge from a technological viewpoint[1058]. In addition, organisational interoperability requires that separated business processes be aligned while using equivalent technology, and legal interoperability ensures that organisations that operate under different legal frameworks are able to work together, avoiding barriers on data processing[1059].

The EHR is primarily used for patient care delivery and patient care management, but it is useful for patient care support processes, financial and other administrative processes, and patient self-management, too[1060]. Previous research has established some requirements or attributes of the EHR, which may be listed as follows[1061]:

– "accessibility and availability", meaning the EHR allows continuous access to patient data or timely access to other information sources;
– "reliability", meaning the EHR ensures data integrity and the permanence of original information in an agreed format and for a given period of time;
– "usability and flexibility", meaning the EHR supports multiple user views and user- friendly interactions with the system;
– "integration", meaning the EHR enables the integration of different administrative and clinical information systems (CIS), e.g. from the pharmacy to the hospital;

1057 *See* Shabo, "Electronic Health Record".
1058 Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", p. 109.
1059 *See* EC European Commission. *New European Interoperability Framework, Promoting seamless services and data flows for European public administrations*. European Commission. Luxembourg: Publications Office of the European Union, 2017, pp. 25, 27.
1060 *See* Stephen P. Julien. "Electronic Health Records". In: *Public Health Informatics and Information Systems*. Springer, 2014, pp. 174–190. ISBN: 9780387227450. The author studied the technology in the US framework, but the uses concern the functionalities outlined above for the EU legal framework, too.
1061 Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", p. 107.
1062 On query and surveillance systems *see* James J. Cimino and Edward H. Shortliffe. *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*. Springer-Verlag, 2006. ISBN: 9780387289861, p. 466.

– "performance", meaning the EHR ensures the provision of information normally within a few seconds, through query and surveillance systems[1062];
– "confidentiality and auditability", meaning the EHR normally provides an audit trail which documents the interactions with the system (i.e. user access), and uses authentication and authorisation systems for access control.

The concept of EHR is evidently connected with the clinical information system (CIS) of the healthcare provider. Since the first arrival of computers in the medical environment, hospitals developed hospital information systems (HIS) to use these technologies in all healthcare processes[1063]. In the 2000s, the use of networks allows the development of EHR solutions. The CIS is the subset of the HIS that is directly devoted to patient care[1064]. At the core of the CIS is the EHR, as the system for recording data collected in the hospital. A similar description can be provided for a private clinic. It has been highlighted that EHR is often used as synonym of CIS, but they are different systems since the EHR is a component of the CIS, which allows the integrated recording and access to patients' data[1065].

The literature classifies five functional components of an EHR that are typically implemented[1066].

1. Integrated view of a patient's data, e.g. medical history, or diagnoses, from different sources;
2. Clinical decision support system, which is a system for assisting the decision-making process of the user, e.g. a physician or a specialist[1067];

1063 *See* P. Degoulet, D. Luna, and F.G.B. de Quiros. "Clinical information systems". In: *Global Health Informatics*. Elsevier, 2017, pp. 129–151. ISBN: 9780128045916, p. 129.

1064 *Ibid.*

1065 *See* Degoulet, Luna, and Quiros, *op. cit.*, p. 132. This contribution provides a description of some CIS and EHR projects in Brazil and France.

1066 *See* Cimino and Shortliffe, *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*, p. 452; Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*. On the functional model *see* also Nicolas P. Terry. "Electronic health records: international, structural and legal perspectives". In: *Journal of Legal Medicine* 12.1 (2004), pp. 26–39.

1067 *See* Reed T Sutton et al. "An overview of clinical decision support systems: benefits, risks, and strategies for success". In: *NPJ Digital Medicine* 3.1 (2020), pp. 1–10, which provides a valuable definition: "clinical decision support system (CDSS) is intended to improve healthcare delivery by enhancing medical decisions with targeted clinical knowledge, patient information, and other health information. A traditional CDSS is comprised of software designed to be a direct aid to clinical decision making, in which the characteristics of

3. Clinician order entry, which helps the user in the order-entry process of information, e.g. of prescriptions or medications;
4. Access to multiple knowledge resources, such as images from laboratory results or radiology tests, which were previously isolated;
5. Integrated communication and reporting support, which allows the electronic integration of messages to a patient's record, and the notifications of medical results.

Source systems have a supporting infrastructure for their integration and data aggregation, and the clinical data repository (CDR) consolidates data from the sources, as a database[1068]. The interface of the EHR has a presentation layer that allows data entry and query for each patient. The EHR network allows the Health Information Exchange (HIE) between entities[1069]. Finally, the EHR storage system provides all the collected and integrated data.

The platforms may be distributed, and may be released by different vendors or developed independently[1070]. Usually, the EHR implementation is devoted to private companies, who sell or licence the product to healthcare providers. Clinical information systems often store data in proprietary formats[1071]. For these reasons, several standards have been developed for the EHR implementation, for clinical vocabulary, for data formats, for the communication of the record, for interoperability, and for the security features[1072]. As will be discussed in Chapter 5 Section 5.5, internationally recognised standards are widely used in the implementation of EHRs.

Compared to the paper-based record, the EHR is flexible and adaptable since the data are entered in some formats, and then displayed in other formats suitable for their interpretation; and data which were previously separated from the record, such as multimedia information, can now be

---

an individual patient are matched to a computerized clinical knowledge base and patient-specific assessments or recommendations are then presented to the clinician for a decision".

1068 *See* Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, p. 35.

1069 *See* Guarda, *op. cit.*, p. 36.

1070 *See* Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*.

1071 *See* Aceto, Persico, and Pescapé, "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges", p. 132.

1072 *See* Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", p. 110; Sinha et al., *Electronic health record: standards, coding systems, frameworks, and infrastructures*, p. 8.

integrated with it[1073]. Data entry evidently may require more time than before, since the user should record the information through electronic interfaces in the system or scanning[1074]. The data are stored in a database and are accessible by remote access in the network. The same data are more legible and complete than the paper-based data since they are written in machine-readable form, there are multiple formats, and the system can even indicate the additional information to be added for the user[1075]. However, the EHR implies more costs than the paper-based record because it requires more technical, organisational and human factors. As the data are stored in digital form, the computer system might fail; therefore, systems should have disaster recovery plans[1076]. Users may be trained to use the system and the organisation should determine authorised users upfront. It has been highlighted that the implementation of the EHR may be slow and expensive and may bring about usability problems[1077]. At the same time, many projects over the years have focused on EHR technology, and provided good solutions[1078].

In 2018, a detailed study commissioned by the European Commission to DG Communications Networks, Content & Technology showed the common personal health data of EHR systems at the EU level. The data available in more than 90 % of cases or used in more than 80 % of them are listed as follows: "medication list; prescriptions and medications; basic medical parameters; problem list and diagnoses; immunisations; medical history; lab test results; symptoms reported by the patient; ordered tests; and clinical notes"[1079]. Other possible frequent data are: "treatment outcomes, administrative patient's data, patient's demographics, finances or billing data, and radiology test reports or images"[1080]. This information

1073 *See* Cimino and Shortliffe, *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*, p. 448.

1074 *See* Cimino and Shortliffe, *op. cit.*, pp. 463–464.

1075 *See* Cimino and Shortliffe, *op. cit.*, pp. 449, 466.

1076 *See* Cimino and Shortliffe, *op. cit.*, p. 450.

1077 Quintana and Safran, "Global health informatics — an overview", p. 4.

1078 *See* e.g. the comparison by Terry, "Electronic health records: international, structural and legal perspectives". *See* also the work of the openEHR Foundation. An overview is provided by Dipak Kalra, Thomas Beale, and Sam Heard. "The openEHR foundation". In: *Studies in health technology and informatics* 115 (2005), pp. 153–173.

1079 *See* Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*, p. 51.

1080 *See ibid.* Examples of documentation are also provided by the literature. According to Hartley, "information includes the chief complaint (or reason

represents the common core of data of the EHR. It is worth highlighting that the EHR typically collects both medical data and common personal data. Excluding financial and billing data, the other personal data can easily fall under the definition of data concerning health of the GDPR. So, the data have been combined by the eHealth Network with the functionalities available in the EHRs, as reported in the following Table 3.5[1081].

Table 3.5 EHR overview: sub-dimensions and functionalities

SUB-DIMENSION	FUNCTIONALITIES
Integrated view of Health data	Symptoms, reason for appointment, clinical notes, vital signs, treatment outcomes, medical history, basic medical parameters (e.g. allergies), problem list/diagnoses
Clinical Decision Support System	Contraindications, drug-drug interactions, drug-lab interactions, drug-allergy alerts, clinical guidelines and best practices, being alerted to a critical laboratory value

for visit) that the patient self-reports, the patient's past medical history, the patient's family and social history, and details of the physician's physical exam and findings (or problem list), assessment, and treatment plan. The treatment plan may include preventative measures, such as an annual exam or mammogram, and it may include treatment for an acute disease or life-long treatment for the management of a chronic disease. Also included are copies of faxes, signed permissions and consent forms, lab results, imaging reports, and other information provided by the patient. Unlike the paper chart, however, the EHR is a secure, real-time, interoperable point-of-care, patient-centric information resource for clinicians. Lab results can be posted into an electronic flow sheet, which is especially important for care managers tracking the patient's trends. The EHR also provides immediate access to the patient's current medications and closes loops in communication and response that result in delays or gaps in care, such as with billing, quality management, outcomes reporting, resource planning, and public health disease surveillance". *See* Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 3.

1081 *See* Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*, p. 59. The sub-dimensions have been aligned to the description provided above on the five typical functional components.

SUB-DIMENSION	FUNCTIONALITIES
Clinical Order-Entry and Result Management	Medication list, prescriptions/medications, immunisations, lab test results, ordered tests
Access to Image	Radiology test images, radiology test reports
Integrated support with administrative data	Finances/billing, administrative patient data

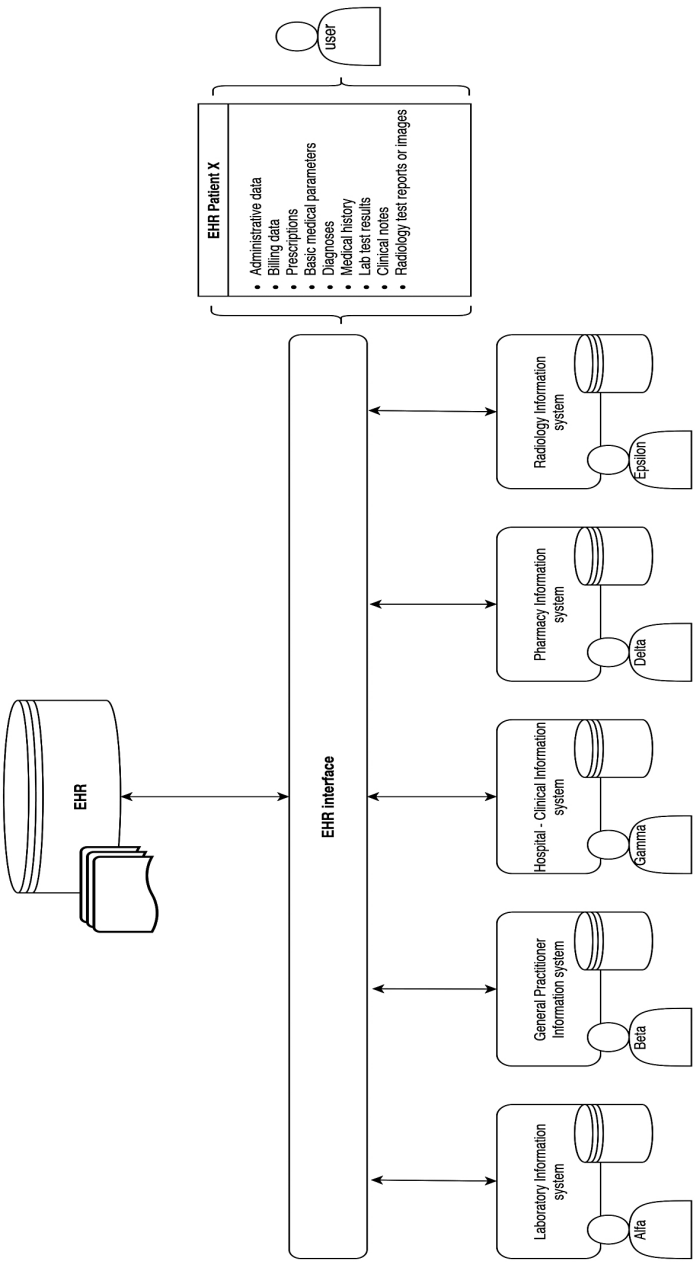
In sum, different components of source systems and clinical information systems store and archive valuable personal health and common data useful for the patient's care, and are connected in a network for supplying the same data in the EHR system[1082]. Three functions of the EHR may be grouped: the storage with the data at rest; the network where the data are transferred; and the computation area where the data are used[1083]. The access level of the users on the software application will be defined at the policy level through privacy access control. A typical EHR concept overview may be schematised as reported in Figure 3.1[1084].

1082 Cimino and Shortliffe, *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*.

1083 For the typical ICT areas and the three data states *see* Matthijs Koot and Cees de Laat. "Privacy from an Informatics Perspective". In: *The Handbook of Privacy Studies: an Interdisciplinary Introduction*. Amsterdam University Press, 2019, pp. 213–255. ISBN: 9789462988095. According to the authors, "being aware of these three states helps grasp data and communications privacy from an informatics perspective, including potential threats to privacy and countermeasures to protect against such threats".

1084 Own graphic inspired by: Corporation MITRE. *Electronic Health Records Overview*. National Institutes of Health National, Center for Research Resources. 2006, p. 5; Bieber, Richards, and Walker, *Implementing an electronic health record system*, p. 90; Cimino and Shortliffe, *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*, p. 453.

Figure 3.1 EHR concept overview



The privacy and confidentiality issues change when data are stored in electronic form[1085]. The EHR system must confront confidentiality, data protection and security principles and obligations. The next section discusses the EU legal framework applicable to the processing of data in the EHR systems.

3.4.2 The data protection framework for EHRs

The EHR is currently available and adopted in all Member States[1086]. At the EU level the data protection framework for EHRs is set out by Article 8 of the EU Charter of

Fundamental Rights, by the GDPR, and by Directive 2011/24/EU on patients' rights in cross-border healthcare[1087]. Regulation 910/2014 on electronic identification may also apply in the EHR context for guaranteeing secure electronic signatures, electronic identification and authentication of individuals in the system, while Directive 2016/1148 on security of network and information systems and its national transpositions establish other rules[1088]. The processing in the EHR should comply with the rules laid down in Article 8 of ECHR, the CoE Convention, CoE Recommendation No. R(97) 5, and CoE Recommendation CM/Rec (2019) 2[1089].

1085 *See* e.g. Terry, "Electronic health records: international, structural and legal perspectives"; Liesje De- muynck and Bart De Decker. "Privacy-preserving electronic health records". In: *IFIP International Conference on Communications and Multimedia Security*. Springer. 2005, pp. 150–159.

1086 *See* the detailed report by Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*.

1087 Therefore, the framework outlined in Section 3.3 applies here. In this context Directive 2011/24/EU provides the rules for the cross-border use of EHRs, as will be further discussed in the next section.

1088 *See* EC European Commission. *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*. European Commission. Brussels: COM (2019) 800 final, 2019, p. 3. *See* also the text of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. O.J. L. 257, 28.8.2014.

1089 All these rules are described in Section 3.3. In 2007 the WP29 listed the data protection framework applicable for EHR: Article 8 of ECHR; Article 8 of the EU Charter of Fundamental Rights; DPD; Directive 2002/58/EC on privacy and electronic communication; national laws of the Member States implementing these two Directives; rules laid down in the Council of Euro-

In addition to this general framework, every Member State can provide for specific rules on the EHR[1090]. It has been reported that health records have been regulated in the different Member States through healthcare laws, legislation on patients' rights and general legal rules and guidelines on privacy and protection of personal health data[1091].

As an example, in Italy Legislative Decree no. 179/2012 created the framework for the use of the EHR at the national level and defined this tool as "the set of data and digital documents relating to social and health information generated by present and past clinical events about the patient"[1092]. The Italian EHR may be populated by all subjects of the NHS at a regional level that are involved patient care, including the same patient in some cases[1093]. In 2009, the Italian DPA released some guidelines on

---

pe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181); Council of Europe Recommendation No. R(97) 5 on the protection of medical data (13 February 1997). *See* Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, p. 6.

1090 For a legal analysis of the legal framework before the GDPR and under the DPD *see* Jos Dumortier and Griet Verhenneman. "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed". In: *ICRI Research Paper, Interdisciplinary Centre for Law and ICT, K.U. Leuven* 5 (2011). *See* also the detailed report by Ltd. Milieu and Time.lex. *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*. Brussels: 201/65. 2014. This study was mandated by the European Commission and it analysed the 28 Member States' legal framework in order to identify the rules on EHR and the existing legal barriers for cross-border access to records. The legal research used both legislation and guidelines and recommendations of the national DPAs.

1091 Jos Dumortier and Griet Verhenneman. "Legal regulation of electronic health records: a comparative analysis of Europe and the US". In: *eHealth: Legal, Ethical and Governance Challenges*. Springer, 2013, pp. 25–56. ISBN: 9783642224744, p. 50.

1092 Guarda and Ducato, "From electronic health records to personal health records: emerging legal issues in the Italian regulation of e-health", pp. 273–274.

1093 Guarda and Ducato, *op. cit.*, p. 274. The aim of the patient's contribution is the patient's empowerment. On the Italian EHR *see* also Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*; Faralli, Brighi, Martoni, et al., *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health*, pp. 193–202; Maria Gabriella Virone. *Il Fascicolo Sanitario*

EHR systems providing a list of safeguards to be implemented to protect the right to data protection of Italian patients[1094]. In this legal framework the EHR is instituted by the Regions and Autonomous Provinces for the purposes of care, scientific research in the medical, biomedical, and epidemiological fields, and for public healthcare planning, verification of care quality, and evaluation of health assistance at the governance level.

In France, the *dossier médical partagé* (DMP) stores the medical history of French patients and allows the collection of all other personal health data in specific areas in accordance with the *Code de la Santé publique*[1095]. The

---

Elettronico. Sfide e bilanciamenti tra Semantic Web e diritto alla protezione dei dati personali. Aracne Editrice, Roma, 2015. ISBN: 9788854883840, pp. 84–94; Rossana Ducato. "Database genetici, biobanche e "Health Information Technologies"". In: *Il diritto dell'era digitale*. Il Mulino, Bologna, 2016, pp. 305–320. ISBN: 9788815266170, pp. 315–320; 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"; Licia Califano. "The Electronic Health Record (EHR): Legal framework and issues about personal data protection". In: *Pharmaceuticals Policy and Law* 19.3 – 4 (2017), pp. 141–159; Vergottini and Bottari, *La sanità elettronica*; Carro, Masato, and Parla, *La privacy nella sanità*, pp. 179–194; Farina, *Il cloud computing in ambito sanitario tra security e privacy*, pp. 75–107.

1094 Italian Data Protection Authority, Guidelines on the Electronic Health Record and the Health File. Doc. web. 1672821. G.U. n. 178 of 3.08.2009. For comments on these guidelines *see* Califano, "The Electronic Health Record (EHR): Legal framework and issues about personal data protection".

1095 The rules are defined in the Code at Articles L.1111 – 14 – L.1111 – 21, R.1111 – 26 – R.1111 – 43 L.1110 – 4, R.1110 – 1. *See* the Code at <www.legifrance.gouv.fr/affichCode.do?cidTexte= LEGITEXT000006072665>; the DMP's official website at <www.dmp.fr>; and the CNIL portal at <www.cnil.fr/fr/dossier-medical-partage-dmp-questions-reponses>. Last accessed 06/10/2021. According to the official website, the DMP is organised into nine specific areas: a summary record, one for treatments, one for analyses, one for reports, one for imaging, one for certificates and one for prevention. On the *dossier see* e.g. Richard Pougnet and L. Pougnet. "Le dossier médical partagé: pour un usage centré sur la personne?" In: *Éthique & Santé* 16.2 (2019), pp. 64–70; Jacques Lucas. "Le partage des données personnelles de santé dans les usages du numérique en santé l'épreuve du consentement exprès de la personne". In: *Ethics, Medicine and Public Health* 3.1 (2017), pp. 10–18; Nathalie Devillier. "Les dispositions de la loi de modernisation de notre système de santé relatives aux données de santé". In: *Journal International de Bioéthique et d'Éthique des Sciences* 28.3 (2017), pp. 57–123; Valérie Siranyan. "La protection des données personnelles des patients face à la modernisation de notre système de santé". In: *Médecine & Droit* 158 (2019), pp. 112–117. Before 2016, the dossier was called *dossier médical personnel*. On this dossier *See* Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 65–70.

dossier is populated by all professionals entitled to the patient's treatment. In Luxembourg, the EHR is called *Dossier de Soins Partagé* (DSP), and the services are grouped with the term eSanté[1096]. In 2019 the Luxembourgian DPA, the *Commission nationale pour la protection des données*, released a document on the protection of personal health data in the DSP and the applicable national law[1097]. So, these few examples show that a Member State usually establishes rules on EHR at a national level. Nevertheless, for the protection of personal data the general rules are still provided by the GDPR.

It has been argued that the legal definition of EHR should take into account two elements. On the one hand, the EHR may store in an electronic form all data previously stored on paper; on the other hand, the EHR may allow the sharing of data with all the entitled parties involved in the patient's treatment[1098]. At the EU level, the EHR has been defined by Article 29 Working Party as[1099]:

> "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".

The legal definition has been framed by the "Working Document on the processing of personal data relating to health in electronic health records (EHR)" issued by WP29 in 2007. This document provided guidance on the applicable legal framework for EHR systems by establishing some general

---

1096 The rules are provided by Loi du 24 juillet 2014 "relative aux droits et obligations du patient, portant création d'un service national d'information et de médiation dans le domaine de la santé". The official portal is available at <www.esante.lu/portal/fr/espace-professionnel/my-dsp,140,196.html>. The EHR environment in Luxembourg has been schematised as reported at <www.esante.lu/portal/fr/agence-esante/la-plateforme-esante-et-ses-services/schema,397,428.html>. Last accessed 06/10/2021.

1097 *See* Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé, Délibération n° 51/2019 du 18.10.2019 at <cnpd.public.lu/dam-assets/fr/decisions-avis/2019/51-DSP.pdf>. Last accessed 06/10/2021. On this topic *see* also Délibération n 242/2018 du 5 avril 2018.

1098 Guarda, "Biobanks and electronic health records: open issues", p. 133.

1099 Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*.

principles and safeguards[1100]. It should be noted that the definition of EHR refers to the "medical treatment and other closely related purposes" for indicating the purposes of Article 8(3) of the DPD, meaning the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, where the data are processed by a health professional or by an equivalent person[1101]. The GDPR adds the purposes listed in Article 9(2)(h), which include occupational medicine, and the assessment of the working capacity and processing of social care systems as explained above. So, even at a legal level the EHR is mainly a tool for supporting healthcare delivery and processes. Actually, the data in the EHRs may even be used for substantial public interest, public interest in the area of public health, or secondary research purposes in accordance with Article 89 of the GDPR, and so Union or Member State law provides the safeguards for rights and freedoms of data subjects[1102].

Generally, EHR systems can be centralised at a national level or decentralised at a local level[1103]. In 2021, it has been reported that 20 Member States have one national system, 11 Member States have several (national or local) systems and four states have no specific rules[1104]. The EHR system can be either used by one HIS, or by a group of hospitals and primary care systems in a regional or local network, while achieving the continuity of care in the NHS[1105]. Each subject has its own information structure in

1100 *See* the comment on this source by Guarda, "Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context", p. 13.

1101 *See* the footnote specification n. 3 of Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, p. 4.

1102 In 2014, more than a half of the Member States had a specific law on secondary use of personal health data, which may also refer to data in the EHR. So, safeguards such as anonymisation were required. *See* further in Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, pp. 46–48.

1103 In Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", the author provides a comparative analysis on the solutions of the different Member States.

1104 *See* DG Health and Food Security. *Assessment of the EU Member States' rules on health data in the light of the GDPR*, p. 37.

1105 *See* Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", pp. 105–106.

which to process the data, but it is connected with the EHR. Potentially, multiple users can access the EHR system since different subjects interact in the data repository. The data processing entails activities with data in rest (e.g. recording, structuring, storage), data in use (e.g. collection, use, consultation), and data in transit (e.g. transmission, making available)[1106].

This structure makes "patient's data more readily available to a wider circle of recipients than before"[1107]. Therefore, data protection and confidentiality concerns are significant, and should be examined here[1108]. Indeed, the EHR goes beyond the fiduciary relationship between physician and patient, as described above. The analysis focuses on the roles in processing, the legitimate grounds, the necessary data protection safeguards for the national legal frameworks, and the rights and duties in the EHR environment.

Firstly, it is necessary to clarify the subjects and their roles in the processing of personal data. Each healthcare provider or pharmacist has its own purpose (i.e. provision of care or selling drugs) and usually determines its own means of processing (e.g. the system). Therefore, in the EHR environment there might be as many data controllers as there are actors involved[1109]. It is worth pointing out that the users of EHR systems (e.g. physicians, professionals, general practitioners) as access points may be delegated by the data controller (i.e. the healthcare entity, such as the hospital or the clinic) to process the data[1110]. The controller may use processors to carry out some processing operations. Whether the EHR implementation and functions are devoted to private companies, which sell or licence the product to healthcare providers, these entities may be designated as processor by a contract in accordance with Article 28 GDPR.

1106 The examples of activities recall the wording of Article 4 GDPR, whereas the distinction refers to the three types of data state.

1107 Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, p. 5.

1108 *See* the discussion from an ethical point of view in Akhil Shenoy and Jacob M. Appel. "Safeguarding confidentiality in electronic health records". In: *Cambridge Quarterly of Healthcare Ethics* 26.2 (2017), pp. 337–341. This article also presents some potential safeguards in order to foster confidentiality.

1109 *See* e.g. Figure 3.1. That overview represents a decentralised environment because each provider stores the data-keeping record.

1110 It is arguable whether they may be considered recipients in accordance with Article 4(9) GDPR. Actually, they do not receive data by transmission, but directly perform processing activities. So, they concretely process the data in the EHR.

In an EHR environment the data controllers may be both the hospital, and the pharmacy, the clinic, or an individual private professional (a general practitioner), who collect the data – e.g. during a treatment, or a specific examination – process the data, and store them in the EHR storage system. Usually, they are not joint controllers because they do not fall under the definition of Article 26 GDPR: they do not determine the purposes and means jointly. However, they may jointly determine purposes and means in a more coordinated EHR environment[1111]. They all shall comply with the data protection principles of Article 5 GDPR.

Nevertheless, in an even more centralised EHR environment, one central institution controls the whole system and becomes the sole data controller that delegates the processing operations to different entities, i.e. processors[1112].

Secondly, some considerations on the legitimate ground of the processing should be made. As reported above, the definition of WP29 mentioned the "healthcare legitimate ground" of the DPD, which excluded the consent of the data subject. Actually, the authority explained that it is misleading to seek consent when the healthcare service is legitimised by an explicit derogation to the general prohibition on processing sensitive data[1113]. Nevertheless, it has been specified that for the creation of the patient's profile on the EHR system the explicit consent of this data subject may be necessary[1114]. The consent should also aim to indicate which personal health data can be collected and stored in the EHR, and who may have access to them[1115]. Remarkably, the patient can withdraw consent at any

1111 As an example, the Luxembourgian DPA specified that the data controller is not only the national central health authority, but also the entities involved in the treatment since different actors assume different responsibilities for the treatment and, therefore the processing. Thus, they are joint controllers. *See supra* Délibération n° 51/2019 du 18. 10.2019, p. 3. On the joint controllership in an EHR environment *see* also Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 114–116.

1112 The description of centralised or decentralised storage is also provided by Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, p. 17: "EHR as a system furnishing access to medical records kept by the health care professional, who has the obligation to keep records on the treatment of his patients – this is often called decentralised storage, or EHR as a uniform system of storage, to which medical professionals have to transfer their documentation; this is often called centralised storage".

1113 *See* the argument in Article 29 Working Party, *op. cit.*, p. 8.

1114 *See* Carro, Masato, and Parla, *La privacy nella sanità*, p. 189.

1115 *Ibid.*

time. If this happens, the patient's profile in the EHR shall be disabled, and the processing of personal health data will continue on a limited level outside the system.

However, it should be claimed that under the GDPR the processing of personal health data in the EHR may be carried out without consent in accordance with the "healthcare exception". It applies when the data are necessary for the purposes listed in that provision, and the processing is performed by a healthcare professional or a person subject to professional secrecy[1116]. It should also be noted that at the Member State level national law may specify the requirement establishing the consent provision or another legal basis for processing in the EHR[1117]. The Member State has this power in accordance with Article 9(4) GDPR, and the DPD provided for a similar derogation as well[1118]. It has been claimed that this discretion

---

1116 *See infra* Section 3.3.2.

1117 In 2014, Member States had different approaches, which could be divided into three groups: some states required consent for the creation of the EHR and the inclusion of data; others required consent for inclusion only; finally, no consent was required in the residual Member States. *See* Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, pp. 32–33.

1118 In Italy, according to national law D.L. 18 Ottobre 2012 n. 179, art. 12 co. 5, the consent of data subject was necessary for the collection of the data in the EHR (i.e. the feeding of the EHR), the connections between providers and the access level of the professionals. In the COVID-19 crisis, D.L. 19 maggio 2020 n. 34 repealed Article 12, deleting the necessary consent. The Italian DPA has highlighted that for healthcare purposes consent is not necessary for the processing, but for the EHR processing the consent is still necessary under Italian law for the access level of the professionals in order to guarantee the right to self-determination of the patient. *See* the Doc-Web 9091942 of March 7 2019 at <www.garanteprivacy.it/ home/docweb/-/docweb-display/docweb/9091942>, and the Doc-Web 9351203 of May 25 2020 at <www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9351203>. Last accessed 06/10/2021. A comment on this guidance is provided by Massimo Foglia. "Patients and Privacy: GDPR Compliance for Healthcare Organizations". In: *European Journal of Privacy Law & Technologies* (Special issue 2020), pp. 43–50. In France, in accordance with Décret n°2016–914 du 4 Juillet 2016 and the *Code de la Santé publique*, consent is necessary for the creation of the DMP and for the access level of the professionals. *See* at <www.dmp.fr/patient/faq>. Last accessed 06/10/2021. The *décret* is available at <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032842901&dateTexte=20200530>. Last accessed 06/10/2021. Other applicable rules are: Articles from L1111–14 to L1111–21, and from R1111–26 to R1111–43 of the *Code de la Santé publique*. According to the CNIL, the retention of medical information is based on a

reserved to Member States may create some obstacles for EHR that may impinge on access to safe and high-quality cross-border healthcare which is strongly promoted by the EU with Directive 2011/24[1119]. Where national law does not provide a specific rule, Article 9(2)(h) GDPR may be a lawful legal basis for the collection of data in the EHR system.

For non-medical staff in the EHR network national law may lay down binding rules to ensure an equivalent level of confidentiality, which allows the application of the "healthcare exception"[1120]. Whether or not the conditions of Article 9(2)(h) and 9(3) GDPR are applicable – e.g. the purpose goes beyond the medical treatment, there is not an obligation of confidentiality or secrecy – the processing shall seek another legitimate exception[1121]. Anyway, it is questionable whether the explicit consent

---

legal obligation. *See* CNIL. Commission Nationale de l'Informatique et des Libertés. *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*. 2020. On November 2020 Liechtenstein notified the proposal "Act of... on electronic health records (EGDG)" to the European Commission. Liechtenstein participates in the European Economic Area and so the GDPR applies there. The Act states that "the electronic health records fulfil a substantial public interest within the meaning of Article 9(2)(g) to (j) of Regulation (EU) 2016/679". So, this Act will be the Liechtenstein law pursuant to Article 9(2)(g), (h), (i), (j) GDPR. This Act establishes the applicable rules for the data processing, including subjects, content, principles and rights. It will enter into force "on 01 January 2022 if a referendum is not called within the statutory period, and otherwise on the day after its proclamation" (Article 21).

1119 *See* Califano, "The Electronic Health Record (EHR): Legal framework and issues about personal data protection", p. 148.

1120 This proposition was made in the Working Document by the WP29 under the DPD for allowing the application of this exception.

1121 In fact, in the Working Document on EHR the WP29 stated interestingly: "If the question were raised whether Article 8(3) of the Directive could serve as the sole legal basis for the processing of personal data in an EHR system, the Article 29 Working Party is of the opinion that Article 8(3) could only pertain to the processing of medical data for strictly those medical and health-care purposes mentioned therein, and strictly under the conditions that processing is "required" and done by a health professional or by another person subject to an obligation of professional or equivalent secrecy. Where the processing of personal data in an EHR goes in any way beyond these purposes or does not meet the said conditions, then Article 8(3) cannot serve as the sole legal basis for the processing of that personal data". And also: "The main and traditional safeguard in Art. 8(3) – apart from the purpose limitation and the strict necessity requirement – is the obligation of medical professionals to confidentiality concerning medical data about their patients. This may no longer be fully

of the data subject may provide more safeguards than other legitimate grounds[1122].

Consent may instead be an appropriate source of legitimisation of the access to data by health professionals. It expresses the informational self-determination of the patient. Applying the principle of control over personal health data, the patient needs to know with whom the data are shared[1123]. So, the EHR may be available without consent in order to simplify the processing activities related to the treatment, but consent may be necessary to establish which other category of professionals or which other entity in the network may access the repository[1124].

In an exceptional situation, where the other grounds do not apply, the protection of the vital interest of the data subject or another person may legitimate the processing in the context of the EHR[1125]. Additionally,

---

applicable in an EHR environment, as one of the purposes of EHR is to grant access to medical documentation".

1122 As an example, consent will be necessary for automated processing which is not strictly related to a healthcare purpose, or in the AI and Big Data environment where the EHR may be used for predictions and inferences beyond the traditional healthcare treatment.

1123 *See* Koelewijn, "Privacy from a Medical Perspective". The author reported three principles for informational medical privacy: control over data, subsidiary principle, and purpose limitation principle.

1124 This is the approach presented by the Italian DPA in the Doc-Web 9351203 of May 25 2020 (*see supra* note no. 1118): "In particolare, è stata ritenuta opportuna – e dall'Autorità condivisa – l'eliminazione del consenso all'alimentazione del Fascicolo, confermando invece quello (autenticamente espressivo di autodeterminazione informativa) relativo alla consultazione da parte dei professionisti sanitari. Tale modifica contribuisce a semplificare notevolmente il processo di costituzione dell'fse rendendolo quindi automaticamente disponibile a prescindere da manifestazioni di volontà individuali, ma confermando il consenso del paziente quale fonte di legittimazione dell'accesso ai dati, da parte del professionista sanitario. Lo spettro del fascicolo è ampliato, sino a comprendere tutti i documenti, sanitari e socio-sanitari, riferiti alle prestazioni erogate, a carico o meno del SSN, includendo dunque tra i soggetti abilitati all'alimentazione la generalità degli esercenti le professioni sanitarie che seguano il paziente".

1125 WP 29 reported this scenario: "by way of example: assume a data subject has lost consciousness after an accident and cannot give his consent to the necessary disclosure of known allergies. In the context of EHR systems this provision would allow access to information stored in the EHR to a health professional in order to retrieve details on known allergies of the data subject as they might prove decisive for the chosen course of treatment". This example of the authority may be misleading since the processing seems justified by the "healthcare exception" once again.

Member State law may provide the use of EHR in the area of public health, or for a substantial public interest, or for research purposes by providing the appropriate safeguards.

As explained above, the definition of personal health data should include the administrative data processed in the e-health context, such as the number or symbol used to identify the patient. So, following the classification of functionalities of the EHR carried out by the EC (and classified in Table 3.5)[1126], processing with the EHR involves data concerning health in a broad sense, administrative data related to health status, and common personal data and billing data. Only the last category is beyond the scope of the "healthcare exception". Name, surname, contact details, and billing data are common personal data, and the lawfulness of their processing is laid down by Article 6 of the GDPR. Thus, it seems that the lawful grounds may be either performance of the contract between the patient and the healthcare provider, or compliance with a legal obligation to which the provider is subject, or a legitimate interest.

Thirdly, the data protection concerns and necessary safeguards for the EHR are related to the particular structure of the data processing. Under the DPD, WP29 reflected on the suitable legal safeguards necessary to guarantee data protection within an EHR, and indicated 11 recommendations for the creation of rules in the national legal frameworks[1127]. So, the recommendations may be grouped and further elaborated as follows[1128]:

1. The processing in the EHR shall respect the right to self-determination of the patient on when and how data are used in light of Article 8 of the EU Charter and Article 8 of the ECHR. So, processing in the EHR

1126 *See infra* in Section 3.4.1 the description of the study conducted by Lupiáñez-Villanueva et al., *Benchmarking Deployment of Ehealth Among General Practitioners*.

1127 *See* Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, pp. 13–21.

1128 This list is based on the safeguards reported by the WP29, but has been updated and further integrated with an independent legal analysis based on the considerations of the previous sections. Even the order has been changed. The topics of the recommendation of WP29 were listed as follows: "1) Respecting self determination; 2) Identification and authentication of patients and health care professionals; 3) Authorization for accessing EHR in order to read and write in EHR; 4) Use of EHR for other purposes; 5) Organisational structure of an EHR system; 6) Categories of data stored in EHR and modes of their presentation; 7) International transfer of medical records; 8) Data security; 9) Transparency; 10) Liability issues; 11) Control mechanisms for processing data in EHR".

may require both opt-in and opt-out solutions, or rights to refuse[1129]. A national law establishing the use of the EHR should provide both opt-in requirements for choosing whether particularly sensitive personal health data (e.g. abortion, abuse) may be collected in the EHR, and also opt-out requirements for the data subjects. These opt-out requirements should allow the patient to prevent the disclosure to particular healthcare professionals of a category of data or specific data. As a result, the choice of the data subject will be central for processing in the EHR. The right to self-determination may allow the patient to limit the data to be stored and the operations to be performed in the EHR[1130]. However, the data subject should be well-informed on the risks since any choice of limitation may impact the healthcare treatment. In fact, it has been claimed that comprehensive and complete EHRs provide a better overview of a patient's health than incomplete records[1131];

2. The national law could even define the categories of personal data stored in an EHR and how they are presented in the interface[1132]. Only relevant data should be stored in the EHR, and the access points may have different access requirements, especially in the case of particularly sensitive personal health data. National rules may provide exceptions and particular modules with special safeguards[1133];
3. The EHR system should be set with reliable mechanisms and limits for the identification and authentication of healthcare professionals, staff

---

1129 WP29 stated that agreeing to the EHR is different from simply consenting.

1130 This is one fundamental conclusion in Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, p. 220.

1131 *See* Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*.

1132 As an example, Liechtenstein's "Act of... on electronic health records (EGDG)" (*see* note no.1118) includes: "a) administrative data collected by the Office of Health for each insured person; this includes in particular: 1. name and address of the insured person; 2. personal identification number (IDN); 3. other insurance information; b) health data and genetic data of the participant, which are collected in accordance with Articles 5 to 7. 2) The government shall regulate detailed rules for data referred to in paragraph 1(a) by way of regulation" (Article 3). Data that must be stored are "a) letters of referral and medical reports; b) letters of transfer and discharge reports; c) laboratory findings; d) diagnostic imaging findings; and e) medications" (Article 5).

1133 The protection of "particularly sensitive health data" defined above in Section 3.3.1 may be an example.

and patients[1134]. It has been pointed out that in the EHR "data should not only be protected against outsiders, but also against insiders"[1135]. A national law may give guidance on these fundamental aspects[1136]. Internal policies and guidelines should define the methods for identification and authentication in the organisations or institutions since different approaches could be set (e.g. e- signature or smart cards)[1137]. So, any access should be temporary and traceable[1138];

4. Therefore, the EHR system should require authorisation for professionals involved to access the EHR in order to read and elaborate data. Access to the EHR could vary according to the roles of professionals in the patient's treatment, and the patient may have the right to prevent access to the record and to have autonomous access to it. The categories of professionals could be established previously by Member State law[1139]. As an example, a specialist may have access to more data than a general practitioner, and this subject more than a nurse[1140]. As regards this principle, Recommendation CM/Rec (2019) 2 of CoE suggests that whether an electronic medical file is used, "the exchange and sharing of data between health professionals should be limited to the information strictly necessary for the coordination or continuity of care, prevention or medico-social and social monitoring of the indi-

1134 As will be discussed in Chapter 6, these aspects are crucial for a DPbD implementation of the EHR.

1135 Demuynck and De Decker, "Privacy-preserving electronic health records", p. 150.

1136 Once again it is interesting to mention Liechtenstein's solution. The Act of 2020 refers to the provisions of the E-Government Act, limits authorisation to healthcare providers and subjects involved in the medical treatment, and specifies that "government shall regulate the detailed rules for the principles of data processing by way of regulation, in particular with regard to access authorisation" (Article 4).

1137 As for other contexts, an overview of Member States' approaches is provided by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, pp. 36–37.

1138 These two principles are highlighted by Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 222–223.

1139 This is one of the recommendations at the national level by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 10. At the EU level the report explained that an agreement was very difficult to achieve.

1140 *See* Milieu and Time.lex, *op. cit.*, p. 36.

vidual". Access by professionals should be adjusted in accordance with their tasks and authorisations, and measures should be taken to protect the security of the record[1141];

5. The EHR must be set with strict requirements and measures for data security (e.g. PETs). National law may indicate some specific and neutral measures[1142]. It was reported that almost all Member States required encryption of data in the EHR and few countries even established a legal obligation for encryption[1143];
6. National law or internal guidelines should describe the organisational structure of the EHR system, which may be centralised or decentralised at the local, regional (e.g. Italy, Spain) or national (e.g. France) level[1144]. Actually, the structure of the network and storage are fundamental for determining the roles in the processing activity, as discussed above;
7. National law should also provide requirements for transparency at the organisational level of the healthcare service (e.g. notification requirements, or information to the patient);
8. National legal framework should establish the general prohibition from using the EHR for purposes other than the provision of care, such as insurance purposes[1145]. Nevertheless, exceptions and safeguards

---

1141 *See* Article 8.3 and 8.4 of the CoE Recommendation CM/Rec (2019) 2.

1142 As will be discussed in Chapter 6, security aspects are pivotal for the implementation of the EHR.

1143 In 2014 the Member States that required this obligation were Austria, Italy, and Poland. *See* Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 29. In Liechtenstein's Act encryption is indicated as a security measure, but further requirements must be laid down through government regulation (Article 9 on data security). *See* note no. 1118.

1144 *See* Milieu and Time.lex, *op. cit.*, which describes the situation of the Member States in 2014 and DG Health and Food Security. *Assessment of the EU Member States' rules on health data in the light of the GDPR* for 2021.

1145 As discussed in Section 3.3.2, the insurance purposes are outside the scope of the "healthcare exception". Insurance companies will process personal health data for their contracts outside the EHR environment by seeking the explicit consent of the data subjects. Insurance companies should not be recipients of the EHR processing since they cannot guarantee neither the respect of the duty of confidentiality of physicians or the principles related to a healthcare purpose. In Greece, pursuant to Article 23 of Law 4624/2019, data stored in a personal electronic health care record cannot be processed for other purposes, including employment and insurance purposes. *See* also TIPIK, *Report on the implementation of specific provisions of Regulation (EU) 2016/679*, p. 10.

may be laid down by national law for other uses, or a secondary use of personal health data in the EHR for scientific medical research purposes, or other purposes related to a public interest[1146];

9. It is of paramount importance that national law establishes that international transfer out of the EU of EHRs may be performed only in aggregated anonymised or pseudonymised form since this scenario is problematic for the high data protection risks[1147];
10. The legal frameworks should lay down rules for liability where a violation occurs in the EHR environment[1148];
11. Finally, national law should establish control mechanisms for evaluating the safeguards set down for processing in the EHR. WP29 suggested special arbitration procedures, the definition of rules on liability of one entity among the others in the EHR network, and regular internal and external data protection auditing. Independent auditing requirements may attest to the implementation of data protection principles and security policies[1149].

Compliance with these principles may enhance the protection of personal data in the EHR system.

In addition to these aspects, it is worth mentioning the data minimisation principle, which limits processing to the data necessary for the treatment purpose, DPbD and DPbDf obligations, and the accountability principle. According to the data minimisation principle, the data in the EHR should be limited to what is necessary for the healthcare purpose, be adequate and relevant; to this end, pseudonymisation techniques may be

---

1146 CoE Recommendation CM/Rec(2019) 2 specifies that "insurance companies cannot be regarded as recipients authorised to have access to the health-related data of individuals unless law provides for this with appropriate safeguards and in accordance with principle 5" (Article 9.2). Moreover, a specific section of the Recommendation is dedicated to research purposes (Article 15).

1147 In this book the data transfer out of the EU has never been mentioned. The GDPR sets out the rules for transfer in Articles 44–50 by providing specific mechanisms and safeguards. *See* Christopher Kuner. "Chapter V Transfers of Personal Data to Third Countries or International Organisations (Articles 44–50)". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 755–862. ISBN: 9780198826491.

1148 It might even be possible that rules on medical liability (e.g. on negligence) are set for EHRs, but national law should provide for it. *See* the recommendation by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 62.

1149 In some Member States this auditing was even binding. *See* Milieu and Time.lex, *op. cit.*, pp. 29–30.

useful[1150]. The DPbD and DPbDf obligations shall be central in the EHR implementation.

Fourthly, following the considerations in Section 3.3.3 on the relevant provision to comply with in the e-health context, it is worth examining here some aspects on data protection rights and duties in the EHR environment under the GDPR.

As regards the right to be informed, the privacy policy will comply with Articles 13 and 14 GDPR and the information will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language[1151]. In particular, the information on the timing of data storage is fundamental in the EHR context. Storage of the patient's data in the EHR may last a lifetime for healthcare purposes, but may also last for longer in accordance with specific national law, which requires storage for administrative purposes (i.e. general public interest) or even scientific research purposes[1152]. It has been suggested that initial information on the

---

1150 *See* Abedjan et al., "Data science in healthcare: Benefits, challenges and opportunities". In the Guidelines on Article 25, and in particular in the section dedicated to the implementation of the minimisation principle, the EDPB used the following example of EHR: "A hospital is collecting data about its patients in a hospital information system (electronic health record). Hospital staff needs to access patient files to inform their decisions regarding care for and treatment of the patients, and for the documentation of all diagnostic, care and treatment actions taken. By default, access is granted to only those members of the medical staff who are assigned to the treatment of the respective patient in the speciality department she or he is assigned to. The group of people with access to a patient's file is enlarged if other departments or diagnostic units are involved in the treatment. After the patient is discharged, and billing is completed, access is reduced to a small group of employees per speciality department who answer requests for medical information or a consultation made or asked for by other medical service providers upon authorization by the respective patient".

1151 The expressions are borrowed from Article 12 GDPR.

1152 Generally, in this last scenario, data will be pseudonymised or anonymised. As an example of the timing of the storage of personal health data, in Italy the radiology results shall be stored for at least for 10 years (art. 4, D.M. of 14 February 1997). The same timing is established by Act of 24 July 2014 on patients' rights and obligations in Luxembourg. Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, pp. 48–49, reports that usually countries rely on general rules on archiving duration, so the timing is frequently set to ten years. In France, the *dossier médical* shall be retained for 20 years on the basis of Article R. 1112–7 of the *Code de la Santé Publiqu*e. *See* Commission Nationale de l'Informatique et des Libertés,

EHR collection and ordinary operations could be provided immediately, then additional information on other specific processing activities could be provided progressively[1153]. As a result, the data subject may pay more attention to the fundamental information and be made aware of the additional information one later.

The right to access and the right to rectification fully apply to the EHR environment[1154]. As described above, the GDPR mentions medical records in Recital 63 so as to specify that the data subject has the right to access these records in order to be aware of all the information on health treatment. When possible, this access can be executed through remote access to the system[1155]. The data controller should ensure that the EHR can be consulted by the data subject, and that copies of the record can be easily obtained[1156]. The data subject could also have the possibility of knowing who accessed the EHR, even directly online[1157]. It has been claimed that access to the data of the EHR might be mediated by a healthcare professional in order to explain to the patient the significance of the specific

---

Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux, p. 7 and CNIL. Commission Nationale de l'Informatique et des Libertés. *Référentiel des durées de conservation dans le domaine de la santé hors recherche*. 2020.

1153 *See* 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", p. 21.

1154 Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, p. 7.

1155 The study by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 42, specifies that in 2014 more than one third of the Member States allowed the data subject/patient to download the data in the EHR. However, all Member States granted access to the EHRs. In 2021, 20 Member States have an ICT system through which data subjects can access their personal health data. *See* DG Health and Food Security. *Assessment of the EU Member States' rules on health data in the light of the GDPR*, p. 88.

1156 *See* Carro, Masato, and Parla, *La privacy nella sanità*, p. 191.

1157 This possibility is usually set by Member State law. *See* Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, pp. 10, 42–43. As an example, in Liechtenstein's Act of 2020 mentioned above the data subject has the right "to read all of the data contained in the electronic health records", even "by electronic access via the access portal of the eHealth platform or by written notification to the Office of Health" (Article 7).

personal health data[1158]. So, the rationales may be protecting the patient and giving information on the data, but in a concrete digital scenario this mediation is difficult to achieve since the EHR may be accessed by the patient autonomously and by electronic means. Therefore, the personal health data in the record could be associated with a brief explanation by the healthcare professional or could be signalled in a way that suggests seeking medical advice on the same data[1159]. According to the EC, having access to EHR has been shown to improve quality of care and patient safety. If interoperable, given patient mobility, EHRs will also improve conditions for treatment in other Member States, following the rules of Directive 2011/24/EC[1160].

The right to rectification is obviously applicable, but the EHR should contain the versioning of the record for accountability and proofing purposes. Actually, the ability to rectify personal health data with data provided by the patient is questionable. Given the healthcare purposes, the EHR shall contain accurate and high-quality data. So, it has been claimed that, on the one hand, the ability to directly modify personal health data shall be prohibited for the EHR being trustworthy[1161]; and on the other hand, the need to update data in the EHR is based on general rules on data protection, health data and medical ethics[1162]. Whether the data subject

1158 *See* Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 128–129. While commenting on the Italian rules (now repealed by the GDPR), the author explains that mediation is useful for facilitating the comprehensibility of medical data by the patient and for filtering the information in a way that respects the fiduciary relationship between physician and patient. This solution has been criticised by the literature. However, as reported by this source, even the DPD suggested that Member State law could have specified that access to medical data could be obtained only through a health professional (Recital 42). As an example, in France, according to Article L1111–7 of the *Code de la santé publique*, the patient has the option to choose mediation of the healthcare professional or access by himself or herself.

1159 *See* Guarda, *op. cit.*, pp. 131–135.

1160 *See* for these last sentences European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*.

1161 *See* the recommendation by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 10.

1162 *See* Milieu and Time.lex, *op. cit.*, p. 40, which also provides the list of countries where the task of updating EHRs is specifically mandated by law.

has directly inputted some data, the system may allow for him or her to modify this specific data.

Furthermore, as mentioned in Section 3.3.3, the right to erasure has some limits in the healthcare context. In the EHR environment, the law usually requires keeping the data, or the data controller performs public tasks including storing personal data. As a result, personal health data are never erased unless they are processed unlawfully, or a specific provision allows their erasure[1163]. For this reason, and in order to empower the patient, a right of concealment has been established in some legal frameworks to give the patient the power not to reveal to users some data contained in the EHR[1164]. The patient can ask to conceal a data entry in the EHR, and the choice is revocable over time. This personal health data is therefore accessible only to the professional who originally generated it or collected it, or to the patient, and the occurred option of concealment should not be intelligible to other users (so-called "concealment of the concealment")[1165]. Actually, this right has been criticised by healthcare

1163 In this regard, CoE Recommendation CM/Rec (2019) 2 stated that the data subject has the right to erasure of data processed in violation of the provisions of CoE Convention 108 (Article 12.2). It has been reported that few countries allow patients to erase data (Austria and France). *See* Milieu and Time.lex, *op. cit.*, p. 43 and DG Health and Food Security. *Assessment of the EU Member States' rules on health data in the light of the GDPR*, p. 91. In Liechtenstein, data in the EHR are deleted ten years after the expiration of compulsory national insurance (Article 10 of the Act of 2020 on EHR).

1164 In France the patient has the right to "masquage", that is the option to request to hide documents from some health professionals. Nevertheless, the document remains visible to the physician who created it, to the general practitioner and the patient. The choice is revocable anytime. The "masking is masked" since the choice shall not be visible to other professionals. *See* Lucas, "Le partage des données personnelles de santé dans les usages du numérique en santé l'épreuve du consentement exprès de la personne", p. 13. *See* also at <www.dmp.fr/ps/faq>. Last accessed 06/10/2021. In Liechtenstein, the data subject will have the right "to hide or delete health data and genetic data relating to him or her" pursuant to Article 7 of the proposal of Act on EHR of 2020. *See* note no. 1118. In Italy there are comparable rights of "oscuramento" and "oscuramento dell'oscuramento". *See* further the next footnote.

1165 As regards Italy, *see* Califano, "The Electronic Health Record (EHR): Legal framework and issues about personal data protection", p. 156; Guarda and Ducato, "From electronic health records to personal health records: emerging legal issues in the Italian regulation of e-health"; Ducato, "Database genetici, biobanche e "Health Information Technologies"", p. 317; Carro, Masato, and Parla, *La privacy nella sanità*, pp. 190–191; Farina, *Il cloud computing in ambito sanitario tra security e privacy*, p. 84. As reported by the literature, the right of

providers since it limits the EHR potentiality. However, a right of concealment guarantees the right to make free and informed decisions on which data the subject wants to communicate to the physician, and it implies the desire to request the opinion of another specialist without the latter being influenced by the former professional[1166].

Data portability may be useful for guaranteeing treatment in a different EHR environment. However, semantic and technical interoperability limits this right, and it applies only to data provided by the patient and not processed by a public authority[1167].

All the organisational requirements outlined above for the e-health context are necessary in the EHR environment for the same reasons explained there. It is evident that in this context both the likelihood and the gravity can be evaluated as high-level and that personal health data are processed on a large scale. Thus, the record of the processing, the notification and communication of data breaches, the risk assessment with a DPIA, the designation of the DPO and the implementation of organisational and technical measures are usually binding requirements for the EHR[1168]. The present case study then will provide the DPbD set of guidelines with technical and organisational measures for complying with this legal framework in Chapter 6.

As mentioned, EHRs are associated with increased risk of security and data protection. Hence, it is particularly interesting that the first fine for violation of the GDPR was charged to a hospital by the Portuguese Data

---

concealment was firstly proposed by the Italian DPA in its Guidelines of 16 July 2009 (*see supra* note no. 1094). The DPA argued that "without diminishing the definite utility of a complete EHR" it should "be possible to prevent the entry in it of some data concerning health related to individual clinical events (e.g., with reference to the outcome of a specific specialist examination or the prescription of a drug). This is similar to the patient-physician relationship, in which the former can make an informed decision not to inform the latter of certain events". Then, the right to concealment has been established by the first regulatory act approved in accordance with Article 12(7) of D.L. 179/2012.

1166 *See* Califano, "The Electronic Health Record (EHR): Legal framework and issues about personal data protection", p. 156; Claudio Filippi and Melchionna Silvia. "I trattamenti di dati in ambito sanitario". In: *Le nuove frontiere della privacy nelle tecnologie digitali*. Aracne Editrice, 2016, pp. 469–533. ISBN: 9788825507942, p. 493.

1167 On interoperability *see infra* the following section.

1168 Indeed, the EHR system is associated with data protection concerns related to how and by whom the record will be used. Following the WP29 list of principles, specific safeguards should be established.

Protection Authority (CNPD) in December 2018[1169]. The fine amounted to 400,000 euros. The Portuguese DPA sanctioned the hospital for the violation of Article 5(1)(c) and (f) of the GDPR on data minimisation and security. In particular, after an inspection the authority found that the system for patient management was not compliant with these two principles because access to patients' personal data was not limited[1170]. Specifically, the hospital did not implement technical and organisational measures for limiting the identification and authentication of the users in accordance with their profiles and the different levels of access that corresponded to each category of workers[1171]. The security of the personal data was not guaranteed because there was not enough security and an audit system for the access mechanisms was not set[1172]. According to CNPD, the hospital acted freely and voluntarily, and knowing that the conduct was prohibited and punished by the law[1173]. In arguing the decision, the authority described the circumstances in which the information access systems operated and the specific conditions of access with their relative weaknesses[1174]. The system counted 985 users with doctor-level access, but the hospital had only 296 doctors. Access was granted to too many profiles.

Therefore, the hospital violated the principle of data minimisation by allowing indiscriminate access to an excessive set of professionals who should have only accessed in occasional and previously justified cases[1175]. Moreover, the hospital violated the principles of integrity and confidentiality, and Article 32 GDPR on security, by not implementing the technical and organisational measures that should prevent unlawful access to personal data[1176]. When deciding on the amount of the administrative fine the authority gave regard to Articles 25 and 32 of the GDPR by stating that the defendant's responsibility regarding the violation of the restrictions of

1169 *See* the website of the Comissão Nacional de Protecção de Dados at <www.cnpd.pt/english/index_en.htm>. Last accessed 06/10/2021.

1170 The decision is Deliberação n. 984/2018. The decision has not been translated into English, but is available in Portuguese at <www.cnpd.pt/home/decisoes/Delib/20_984_2018.pdf>. Last accessed 06/10/2021.

1171 *See* paragraph 26. In paragraphs 8 – 13, the authority specified that the categories were administrative worker, technician, doctor, computer technician, assistant, surgeon, anaesthetist, nutritionist, physical therapist, psychologist, welfare worker.

1172 *Ibid.*

1173 *Ibid.*

1174 *See* Part IV "Motivação da decisão de facto", pp. 7 and 7v.

1175 *See* p. 7v.

1176 *Ibid.*

the levels of access was high, since it consciously allowed the association of the functional group of "doctors" to whom only a "technician profile" should be granted. It was the responsibility of the hospital to ensure the control of the need or the deletion of the profiles, including through appropriate audit procedures[1177]. The measures were not appropriate for the risks[1178]. It thus can be argued that the risk assessment was not adequate, and that the patient management system was not designed properly.

The case shows that a DPbD approach is not only binding, but also pivotal for a medical record. Following the words of the Italian DPA, in the context of e-health the measures of DPbD and DPbDf are a decisive example of how technology, if supported by a forward-looking "vision" in social as well as legal terms, can represent the solution, instead of the problem, and strengthen citizens' confidence in the health system[1179].

So far, this Chapter has presented the legal framework for personal health data and the case study on the EHR with the state of the art of this technology and the applicable data protection rules. The next section deals with cross-border processing of data in the EHR environment, where it applies primarily Directive 2011/24/CE.

3.4.3 Cross-border interoperability issues

This section presents the EU interoperability policy and investigates the use of EHRs across Member States for providing healthcare. Cross-border interoperability and secure access to EHR systems abroad raise several data protection issues. So, this part identifies the rules and obligations established by the GDPR that should be taken into account in the context of EHR interoperability across Member States[1180].

As mentioned above, in the "transformation of health and care" policy of the EU agenda access to healthcare and sharing of personal health data are priorities. In recent years EU institutions and Member States

1177 *See* p. 8v.
1178 *See* p. 10.
1179 *See* the text of the Doc-Web 9351203 of 25 May 2020 (*see supra* note no. 1118).
1180 A paper has been published on the main issues of this section, Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union". This section then further elaborates the topic.

have launched projects, initiatives and studies[1181], and made significant investments[1182].

In the past, the EU Council urged Member States to conceive initiatives and strategies enabling interoperability of digital health technologies across the EU[1183]. In this scenario, the EHR has always played an important role. EU institutions have claimed many times the urgent need to make progress on standardisation and interoperability of e-health systems to foster a greater use of these digital tools[1184], and to enable the free flow of patients, products and services in the EU market[1185]. In 2020, the European Commission presented the project on the creation of a common space in the area of health named "European Health Data Space ('EHDS')" within its European strategy for data[1186]. According to the EC, this space will be "essential for advances in preventing, detecting and curing diseases as well as for informed, evidence-based decisions to improve the accessibili-

1181 P. Van Langenhove et al. "eHealth European Interoperability Framework". In: *Vision on eHealth EIF, a study prepared for the European Commission by the Deloitte team* 1 (2013).

1182 See the Health policies in the EU budget (2021–2027) at <ec.europa.eu/health/funding/future_health_budget_en>. Last accessed 06/10/2021. *See* Arak and Wójcik, *Transforming eHealth into a political and economic advantage*.

1183 *See* EU Council, Council of the European Union. *Council Conclusions on Safe and efficient healthcare through eHealth. 2980th Employment, Social Policy, Health and Consumer Affairs Council meeting*. Council of the European Union. Brussels: 1.12.2009, 2009.

1184 *See* European Commission, *Commission Staff Working document accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market*.

1185 *See* European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health – making healthcare better for European citizens: An action Plan for a European e-Health Area*.

1186 *See* European Commission, *Communication from the Commission to the European Parliament, the Euro- pean Council, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data*. The EDPS released a specific opinion on the EHDS: EDPS European Data Protection Supervisor. *Preliminary Opinion 8/2020 on the European Health Data Space*. 2020. According to the EDPS, Article 9(2)(i) and 8j) may be the possible legal grounds for processing operations in the EHDS.

ty, effectiveness and sustainability of the healthcare systems"[1187]. EHRs are included in this vision as fundamental digital tools that improve access to citizens' health data[1188].

In addition, Directive 2011/24/EU on patients' rights in cross-border healthcare fosters the right to access healthcare, and personal health data, in any EU Member State[1189]. In particular, it has been highlighted that this Directive establishes a right to have a medical record and have it accessible across borders for the first time in an act of the EU[1190]. The European Health Insurance Card (EHIC) entitles the patient to obtain the healthcare services by a doctor or a public or NHS-affiliated health facility in another Member State. The Directive also stresses the importance of safeguarding the right to data protection during cross-border healthcare services and the transfer of data[1191].

EHR systems might be interoperable at the EU level for fostering cross-border access to healthcare, but the lack of interoperability between them is still a great barrier to access to personal health data in another Member State[1192]. In the healthcare context, the concept of interoperability has rapidly evolved[1193]. A generic definition of the concept within the context of European public service delivery, is[1194]:

1187 European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data*.

1188 *See* point 4.

1189 A report on the progresses of the Member States is usually provided by the EC. *See* EC European Commission. *Report from the Commission to the European Parliament and the Council on the operation of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare*. European Commission. COM/2018/651 final, 2018, where "e-health" has a specific section.

1190 *See* the analysis by Vergottini and Bottari, *La sanità elettronica*, p. 112, which makes reference to Article 4(2)(f) and Article 5(b) of the Directive. According to these authors, the individual also has the right to file an action before an administrative court.

1191 *See* Recital 25 of Directive 2011/24/EU.

1192 EC European Commission and College of Europe. *Synopsis Report. Consultation: Transformation Health and Care in the Digital Single Market*. Publications Office of the European Union. 2018; European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data*, point 4.

1193 *See* Bernd Blobel. "Interoperable EHR Systems–Challenges, Standards and Solutions". In: *European Journal for Biomedical Informatics* 14.2 (2018), pp. 10–19.

1194 *See* the useful and official glossary at <ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+ Glossary>. Last accessed 06/10/2021.

> "The ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems".

So, as mentioned in Section 3.4.1, interoperability implies a variety of layers. The European Interoperability Framework (EIF) for public services made considerable efforts to promote each level[1195]. The first EC Recommendation on this topic was released in 2008, and was aimed at allowing the exchange and use of data collected in the national EHR between neighbouring and non-neighbouring Member States[1196]. The EC urged interoperability of EHRs at technical, semantic, organisational and legal levels, adding a political layer, which was leveraging investments and adapting policies[1197].

A possible cross-border and interoperable environment of EHR systems can be described as follows. Given a Member State of origin *Alpha* and a Member State of treatment *Beta*, the patient originally from *Alpha* seeks healthcare treatment in *Beta* when she is there on holiday[1198]. The patient summary of her EHR in *Alpha* – i.e. a structured part of the EHR – may be accessed by the healthcare professional in *Beta* to provide better clinical treatment. Other examples of data that interoperability may cover are prescriptions for medications or investigations, examination reports, clinic appointments, which are originally collected in the different national or regional records, but could be interoperable cross-border as well[1199]. In *Beta* the healthcare professional may use the local EHR to generate and collect the diagnosis. The two countries have contact points for the data

---

1195 *See* the projects and studies funded by the EU at <ec.europa.eu/digital-single-market/en/news/ ehealth-studies-overview>. Last accessed on 06/10/2021.

1196 *See* EC European Commission. *Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems*. European Commission. Brussels: COM (2008) 3282 final, 2008.

1197 *See* European Commission, *op. cit.*; Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3.

1198 As mentioned in Section 3.3, Directive 2011/24/CE defines country of origin – country of residence or country that originally lawfully provides healthcare – and country of treatment.

1199 *See* Soceanu, "Managing the Interoperability and Privacy of e-Health Systems as an Interdisciplinary Challenge".

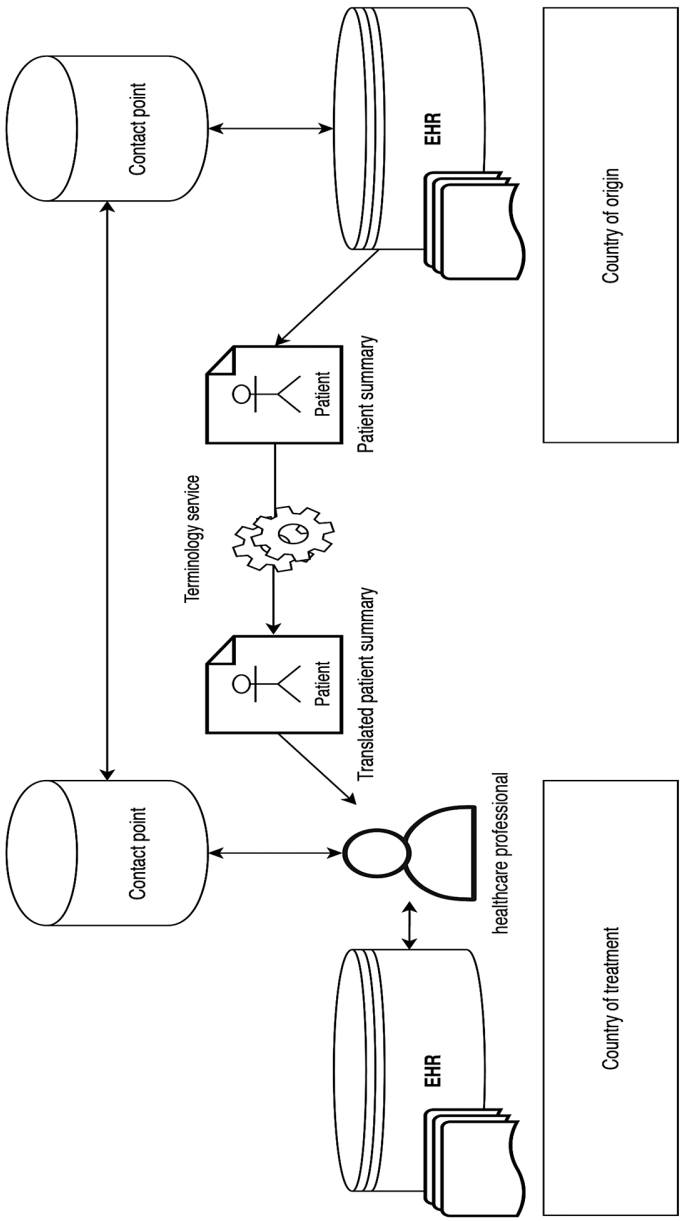
exchange with their respective data repositories[1200]. These points represent the national organisational nodes providing functionalities for the proper and bidirectional working of the network[1201] The following Figure 3.2 is a visualisation of the connections of the network[1202].

1200 As indicated in Section 3.3, Article 6 of the Directive 2011/24/CE allows the designation of one or more national contact points.

1201 The list of contact points is provided at <ec.europa.eu/health/sites/health/files/cross_border_care/docs/ cbhc_ncp_en.pdf>. Last accessed 06/10/2021. For example, in Spain the contact point is the Ministry of Health and in the Netherlands it is the Netherlands NCP Cross-border Healthcare.

1202 Own graphic inspired by the case study by Network eHealth. *Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange in accordance with the cross-border Directive 2011/24/EU*. eHealth Network, 2013, p. 7.

Figure 3.2 EHR interoperability concept overview



As explained in the previous section, Member States may have different specific rules for regulating EHRs. The legal framework is fragmented, but the general rules for data protection are provided by the GDPR. In 2014, before the GDPR, it was reported that only six Member States had provided legal requirements for cross-border exchange and that less than half of the Member States had implemented specific technical rules or standards to achieve this end[1203]. Actually, the vast majority of these countries did not have a framework for the different layers of interoperability and neither national nor EU law established a binding legal requirement in the EHR system implementation to achieve it[1204].

An online public consultation by the EC highlighted the very important need to support EHR interoperability with harmonised standards. In particular, the results of this consultation showed the need for "open exchange formats, common data aggregations and robust EU standards for health data quality, reliability, privacy and cybersecurity"[1205]. It should be clear that interoperability of EHRs does not require uniformity of technologies, and EU rules and policies do not have to impose it[1206], but the existence of different data repositories and several data formats across countries negatively affects cross-border access to personal health data and increases the costs of providing care for NHS[1207].

Actually, EHRs were mostly based on closed proprietary solutions; as a result, in the EU market interoperable and open EHR system solutions were not commonly delivered[1208]. Then, the EU Council called upon the Member States and the Commission to promote the use of interna-

1203 *See* the lengthy study by Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*.

1204 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3.

1205 *See* European Commission and Europe, *Synopsis Report. Consultation: Transformation Health and Care in the Digital Single Market*. The participants even agreed on the need for future EU legislation on these issues.

1206 Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*.

1207 *See* EC European Commission. *Road-map*. European Commission. Ref. Ares (2018) 5986687, 22.11.2018, 2018.

1208 European Commission, *Commission Staff Working document accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market*.

tional and open standards and stressed the need to create common data structures, coding systems and terminologies to improve EHR interoperability[1209]. In order to achieve the different interoperability layers, some conditions may be put in place[1210]:

- a "thorough understanding of the operational environment" of the EHR;
- the identification of "interrelationships and needs" of all the stakeholders;
- the presence of recommendations for concretely "redesigning services and processes";
- supporting "policies for the implementation" of interoperable solutions;
- promoting incentives and availability of adequate resources, including finances and time.

Then, the European e-Health Digital Services Infrastructure (eHDSI) was created by the EC and by the eHealth Network for the cross-border exchange of patient summary and e-prescription tools[1211]. The eHDSI is pivotal for connecting the different EHR environments, and the national contact points[1212].

The EC's Recommendation 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format represented a significant step towards EHR interoperability. In 2018, the European Commission proposed to define recommendations on how EHR systems could be accessed and shared more easily across Member States[1213]. The EC opened a public

1209 *See* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3 on Council of the European Union. *Council conclusions on Health in the Digital Society; making progress in data-driven innovation in the field of health*. Council of the European Union. 2017/C 440/05, 2017.

1210 *See* A. Kouroubalia and D. G. Katehakis. "The new European interoperability framework as a facilitator of digital transformation for citizen empowerment". In: *Journal of Biomedical Informatics* 94 (2019), p. 103166.

1211 As reported by the official website "eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility". *See* <ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home>. See also the description of the eHDSI Mission at <ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/ eHDSI+Mission>. Last accessed 06/10/2021.

1212 *See* also the commentary by Vergottini and Bottari, *La sanità elettronica*, p. 128.

1213 *See* European Commission, *Road-map*.

consultation which showed that EU standard formats for EHR systems would have made access to health data easier for patients, health professionals and other authorised parties using different records across the EU. After the feedback period, the EC released the final version of the Recommendation on EHRs[1214]. Recommendation 2019/243 is aimed at creating a European Electronic Health Record Format by defining the principles that the system should comply with for cross-border interoperability[1215]. The EC framework explicitly includes[1216]:

- the "principles that should govern the access and the exchange" of EHRs across borders;
- a set of "common technical specifications" in certain health information domains (i.e. the baseline for the Exchange Format);
- an organisational process to take forward the further elaboration of the Format.

In detail, this Recommendation establishes wide-ranging technical specifications for secure access to EHRs and their interoperability, and promotes best practices for ensuring data protection and integrity of personal health data. Various technical specifications are indicated as a baseline for future development[1217]. Following the EC words, Member States should ensure high standards in EHR systems for protecting personal health data, and should also secure EHR networks so as to avoid data breaches and minimise security risks[1218]. To this end, Regulation 910/2014 may provide the rules on the secure electronic identification means.

Moreover, Member States should use the digital tools provided by the eHDSI and take appropriate measures to support the use of interoperable EHR systems at policy and legal levels. It should be remembered that the e-Health Network collaborates with Member States to support their e-health policies[1219]. Therefore, the Network is involved in the governance

1214 *See* European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format.*

1215 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 3 on European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*.

1216 European Commission, *op. cit.*, p. 5.

1217 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 4.

1218 *See* European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*, p. 5.

1219 *See* also all the relevant framework in Section 3.3.

processes outlined by the EC, which consist of so-called "national digital health networks". These networks should be set up by Member States by "involving representatives of the relevant competent national authorities and, where appropriate, regional authorities dealing with digital health matters and the interoperability of electronic health records, and security of networks and information systems, and the protection of personal data", including national DPAs[1220]. The rationale is fostering organisational and legal interoperability by governance solutions.

Additionally, the baseline for the European Electronic Health Record Exchange Format provides some interoperability specifications to represent and exchange personal health data in patient summaries, e-prescription and e-dispensation tools, laboratory results, medical imaging and reports and hospital discharge reports[1221]. It is worth noting that these systems collect data which are at the core of EHR systems[1222]. The Commission's Exchange Format will be further improved in the future through a joint coordination process, which will take into account the latest technological and methodological innovations, and will be jointly monitored by the EC and the e-Health Network[1223].

As regards the principles for data processing and data exchange across borders, they are set out in the Annex of the Recommendation[1224]. These principles focus on EHR technical and organisational aspects. It has been argued that "EU citizens should be able to access and securely share their electronic health data across borders, to choose to whom they provide

1220 The EC further specifies that "national digital health networks should involve the following: (a) the national representative of the eHealth Network; (b) national, or regional, authorities with clinical and technical competence for digital health matters; (c) supervisory authorities established under Article 51 of Regulation (EU) 2016/679; (d) competent authorities designated pursuant to Directive (EU) 2016/1148".

1221 *See* European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*, p. 6. The technical specifications will be indicated in Chapter 5 Section 5.5 on EHR standards.

1222 The Recommendation includes even e-prescription and e-dispensation, which are usually separate from the EHR, but can be connected to it in the same local or national network.

1223 *See* European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*, pp. 7–8.

1224 *See* EC European Commission. *Annex to the Commission Recommendation on a European Electronic Health Record exchange format*. European Commission. Brussels: COM (2019) 800 final, 2019, pp. 1–2.

access and the level of detail of the shared health information"[1225]. A high level of data protection shall be guaranteed. The principles can be listed as follows:

- "Citizen-centric by design", meaning that EHR systems should be implemented with DPbD and DPbDf principles so as to place the individual at the centre and comply with the GDPR;
- "Comprehensiveness and machine-readability", meaning that EHRs should be as comprehensive as possible to support an efficient healthcare service, and the data should be stored in machine-readable formats in order to enhance their reuse. Health data should be integrated in interoperable formats;
- "Data protection and confidentiality", meaning that EHRs should be implemented in full compliance with confidentiality rules and data protection law from design stage onward. Particular attention should be paid to transparency, the right to access, and the data subject's other rights;
- "Consent or other lawful basis", meaning that the presence of a legitimate legal basis for the data processing (e.g. a lawful exception) should be always verified;
- "Auditability", meaning that the EHR systems should implement auditing and logging mechanisms for registering and verifying any processing operation;
- "Security", meaning that appropriate technical and organisational measures should be implemented in order to secure EHR systems from security risk, such as "unauthorised or unlawful processing of health data" and "accidental loss, destruction or damage". The users of EHRs should be trained properly so as to be aware of the risks;
- "Identification and authentication", meaning that EHRs should use strong and secure access mechanisms (i.e. identification and authentication). The EC mentions national electronic identification schemes as defined in Regulation 910/2014 for ensuring secure access of citizens;
- "Continuity of service", meaning that the EHR exchange service is necessary to ensure the continuity and availability of care across borders.

Hence, it can be noted that these principles are consistent with the list of principles provided by the WP29 for a national or local EHR. The cross-border processing of data in EHRs requires similar safeguards, which should be adjusted to an even more connected scenario.

1225 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 4.

Even though the Recommendation represents an important step for EHRs, some challenges should be noted here[1226]. In the present legal framework, it will be necessary to remove the residual legal and organisational barriers that exist at Member States' level and to efficiently sustain cooperation across countries[1227]. As indicated above, the EC will monitor the implementation of technical specifications. The responsibility of achieving technical progress remains upon the EHR environment at Member States' level, and therefore upon the market of EHR solutions. Looking at the concrete benefits of the detailed Recommendation, it may be suggested that an EU legislation will better harmonise the standards than the present soft-law approach. However, privacy and data protection concerns are significant.

The cross-border interoperability context increases data protection and security risks because systems are more interconnected than at a national or local level and the amount of personal health data rises, as well as the number of actors involved. Therefore, it is interesting to investigate this context in light of the GDPR by relating the concerns to the respective interoperability layer.

Firstly, legal interoperability requires consistency that avoids the creation and persistence of barriers between legislation of different legal frameworks[1228]. As discussed in this Chapter, the GDPR sets general and consistent requirements for processing of personal health data across the EU. Nonetheless, specific rules for data processing may be established by Member States with possible different regulatory approaches[1229]. Since EHR systems are managed by national or local healthcare providers, the fragmentation of the existing national frameworks may impinge on the legal interoperability layer. Thus, to ensure a "consistent and higher level of data protection"[1230], Member States should define clear interoperability

1226 The challenges were also reported *ibid.*

1227 The first electronic cross-border health service was provided by Luxembourg in 2019. *See* <www. esante.lu/portal/fr/espace-patient/questions-reponses,142,579.html?>. The other 22 countries are reported at <ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en>. Last accessed 06/10/2021.

1228 *See* European Commission, *New European Interoperability Framework, Promoting seamless services and data flows for European public administrations*.

1229 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 5.

1230 *See* Recital 10 GDPR, which suggests an equivalent level of protection through a consistent and high level of protection and the removal of obstacles across Member States.

policies. Legal interoperability could be eased "by ensuring an aligned interpretation of the GDPR provisions and homogeneous applications of data protection principles in all Member States"[1231].

As explained above in Section 3.4.1, organisational interoperability concerns policies, business practices and procedures that should be coordinated to avoid barriers. In the cross-border interoperability context, a patient's data is first processed in a EHR system in a Member State *Alpha*, then it is exchanged and used in another Member State *Beta* for a new treatment or medical consultation. Where personal health data is merely disclosed by transmission from state *Alpha* to *Beta*, the provider in state *Beta* is merely a recipient[1232]. Instead, where in *Beta* the subject accesses the data, uses them, collects medical data of a treatment, and exchanges data in the EHR interoperability network, this subject is an independent data controller which performs processing operations. As a result, two or more data controllers and processors will process the patient's data. It may be argued that they are joint controllers. These controllers may not fall under the definition in Article 26 of the GDPR, since they are independent in the most common scenarios unless a more coordinated environment can be defined (e.g. joint teams for a medical treatment). It could be hypothesised that different Member States will provide rules on the arrangements of joint controllership.

So, all the subjects shall comply with the GDPR and are accountable separately, but as shown by the EC's list above, the implementation of data

---

1231 For this paragraph and the following one, *see* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 5.

1232 As an example, in June 2020 in Malta the cross-border service for patient summary is available for Maltese citizens or residents who travel to Luxembourg, Portugal and Croatia. The privacy policy states that: "who processes and has access to this data? (recipients of personal data) Your Patient Summary data will be accessible only by authorised and identifiable health professionals involved in your treatment, under professional secrecy, in the country of treatment. Each country of treatment participating in the eHDSI system has undertaken to ensure that the participating health professionals and healthcare providers on their territory have adequate information and training about their duties. Details of the participating countries will be published on the eHDSI website. The Patient Summary data will be transferred through a secure technical gateway provided by the eHealth National Contact Point designated by each country. Malta's technical gateway is operated by the Government's IT agency and a private software services company, both of which are bound by strict data protection clauses in their contracts". *See* the privacy policy at <deputyprimeminister.gov.mt/en/imu/cbeh/Pages/Home.aspx>. Last accessed 06/10/2021.

protection principles respects the same safeguards. Thus, the stakeholders could share documentation on cross-border processing to demonstrate compliance. Actually, the contact points of Member States may use the tools of the eHealth Digital Service Infrastructure, as recommended by the EC. The same EC is directly involved in the eHDSI as an EU Institution since it maintains the network for the data exchange. When interoperability is enhanced with the eHDSI, the security of the transmission of personal health data is maintained by the private network that is developed by the EC[1233]. As a consequence, the GDPR applies to Member States, contact points and healthcare providers, whereas Regulation 2018/1725 applies to the EC. In Joint Opinion 1/2019 "on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)", the EDPB and the EDPS jointly argued that the EC is the processor of eHDSI processing operations since it is involved in the development of technical measures[1234].

Beyond the allocation of responsibilities and roles, the presence of the legal basis for cross-border exchange should be investigated. The patient summary in the EHR system is created in one Member State at the local, regional or national level, then it is exchanged in the network thorough the contact points. So, a first legal basis can be identified in *Alpha* in accordance with the rules and conditions described in the previous section. The further processing abroad in *Beta* should be lawful, and so the legal ground should be legitimate as well. Cross-border exchange, access and use of the EHR (and its patient summary) should be possible only if the legal basis of the first Member State is still applicable or another ground applies in the concrete case. In 2014, no Member State required patient consent for cross-border access[1235]. The last EC Recommendation mentions the explicit consent of the citizen concerned or any other lawful

1233 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 5

1234 *See* EDPB European Data Protection Board and EDPS European Data Protection Supervisor. *EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)*. EDPB and EDPS Joint Opinion 1/2019, 2019. Indeed, the EC does not determine the purposes and means of processing, but implements technical measures as processor. Therefore, the EC shall specify its duties in a future "Implementing Act".

1235 *See* Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*.

basis pursuant to Articles 6 and 9 of the GDPR[1236], and some privacy policies now mention consent[1237]. Although it may not be possible to foresee the legitimate ground, it may be suggested that each Member State may provide a legislative basis for the data exchange in accordance with the "healthcare exception" of Article 9(2)(h) or, if necessary, with additional room to manoeuvre of Article 9(4) GDPR.

Moreover, the purpose limitation principle may be circumvented at the organisational level[1238]. Generally, where data in the EHR is collected for healthcare purposes only, no different use is lawful. The secondary use of personal health data for research or scientific purposes will be lawful in accordance with Article 89 of the GDPR. Therefore, a Member State law should provide explicit derogation. The first purpose in the state *Alpha* could even envisage EHR interoperability for medical treatments in the privacy policy. Even so, where the provider in the *Gamma* state is a mere recipient, meaning that personal health data is merely disclosed by transmission from state *Alpha* to *Gamma*, the further processing (i.e. consultation) should be restricted to the limits of the main treatment purpose or should be compatible with it[1239]. Instead, where in *Beta* the subject accesses the data, uses them, collects medical data of a treatment, and exchanges data in the EHR interoperability network, this subject is an independent data controller which performs processing operations. Then, the new controller in *Beta* will organise its own processing activities by determining the purposes, thus finding the specific legal ground and providing the information as prescribed by the GDPR. It has been claimed that the patient should have the opportunity to "opt-out of the data sharing and exchange"[1240].

Since the EC indicated that particular attention should be paid to transparency, data exchange processing should be performed in a transparent

---

1236 *See* European Commission, *Annex to the Commission Recommendation on a European Electronic Health Record exchange format*.

1237 The reference is made to Malta's policy. *See supra* note no.123, where it is specified that interoperability access is available with explicit consent only.

1238 *See* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 6.

1239 The argument follows the definition of the purpose limitation principle of the GDPR.

1240 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*.

manner. The data controllers in both *Alpha* and *Beta* should provide the patient with the relevant and complete information. Thus, it may be recommended that in *Beta* the information should be translated into the native language of the subject or be provided in another language which is well-known to him or her[1241].

Moreover, as discussed for the national EHR environment, it is arguable that a complete DPIA shall be carried out since the risk level is high, a record of the activities should be maintained, a DPO should be designated, and this subject should have knowledge of the data protection concerns on all the different interoperability layers. Thus, joint methodologies on DPIA and records at the EU level could support the stakeholders, who should cooperate with the national DPAs, which are all coordinated in the EDPB[1242]. The assessments may also be made publicly available.

In addition to the legal and organisational layers of cross-border processing, it is now necessary to focus on the data protection issues of the technical aspects emerging in this context[1243]. Cross-border exchange should follow and comply with the principles set out in the GDPR and in the Annex of the EC. Some of these principles are related to the technical development of the EHR, and others to necessary technical and organisational measures to be implemented in processing. Both sources mention storage limitation, confidentiality, security, DPbD and DPbDf. The EC adds comprehensiveness, machine-readability, identification and authentication, and auditability[1244].

As regards the storage of the EHR systems, personal health data collected and stored should be limited to what is "significant for the healthcare purpose" and for the comprehensiveness of the records during cross-border access and use. Even though minimising the amount of data might be complex and interfere with the management of care, it is unavoidable for preventing any misuse in the interoperability context. The data collected should be integrated in interoperable formats, but they should also be accurate and kept up-to-date in all EHR systems in order to support the efficiency of the healthcare service. These systems should be operative for "no longer than what is necessary", meaning that the time limitation on

1241 *See* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 6.
1242 On these last considerations *see* also Bincoletto, *op. cit.*, p. 7.
1243 For the following considerations *see* Bincoletto, *op. cit.*
1244 *See* once again the European Commission, *Annex to the Commission Recommendation on a European Electronic Health Record exchange format*.

the repositories could be agreed among stakeholders, and it should be defined in the privacy policies[1245].

Another aspect in this context relates to access and confidentiality of the record. Firstly, the patient has the right to access the medical record in both *Alpha* and *Beta* in accordance with Directive 2011/24/CE and Article 15 of the GDPR. Actually, access is the main goal of the interoperability policy. As explained for the national EHR environment, the data subject also has the right to know who has accessed the EHR, the right to rectification, and to data portability[1246]. In some Member States, the patient may have the right to concealment, meaning that in *Beta* some data collected in *Alpha* may not be available to the next healthcare provider, and vice-versa. Thus, EHRs' interoperable systems should have the technical functions to execute all the patient's requests for the exercise of data protection rights[1247]. Secondly, in the interoperability context the access mechanisms of healthcare providers – meaning both the professionals and the administrative staff in the state of treatment – should be considered priorities, as shown in the list of principles of WP29. Hence, the access and exchange of data in EHRs should be secure and implemented in full compliance through access control strategies and policies, secure communication chan-

1245 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union" has highlighted that the duration of EHRs archiving is strictly related to the relevance of the collected data and so, it depends on the circumstances. Following the previous example of Malta, the privacy policy states that "in the case of persons domiciled in Malta, the storage period of medical records in Malta is currently for the lifetime of the patient and ten years thereafter, while in the case of other patients, such as persons visiting from other countries, the storage period is ten years". *See supra* note no. 1232. Milieu and Time.lex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report*, p. 64, recommended that the timing should be identical across the EU.

1246 In some contexts where the tasks are carried out as a public interest by way of legislative measure, the right to data portability may not apply. It is interesting to report that in the Preliminary Opinion on the European Health Data Space the EDPS highlighted this limit of application. Despite that, the authority invited the Commission to specify the application of this right in the legislative proposal on EHDS. *See* European Data Protection Supervisor, *Preliminary Opinion 8/2020 on the European Health Data Space*, pp. 13–14.

1247 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 6.

nels and high security standards in order to prevent any unauthorised access[1248].

Interoperable EHRs should then protect the data confidentiality and security of personal health data. Appropriate security measures should be implemented in both contact points, and their EHRs, to prevent data breaches and incidents[1249]. In addition to the security safeguards of the GDPR, as mentioned in Section 3.3, Directive 2016/1148 on security of network and information systems and its national transpositions apply. In particular, in Annex II of this Directive healthcare providers of the interoperability context are listed as operators of essential services which are subject to the requirements of the same Directive and to its national transpositions.

Other common security measures for an interoperable EHR system are auditing, logging of accesses, and back-up mechanisms[1250]. Using harmonised standards for the implementation may ease the compliance of this environment[1251]. Some technical specifications, standards and protocols based on the European Electronic Health Record Format have also been reported by the eHealth Network after the EC Recommendation[1252].

Finally, DPbD obligation must play a major role in the development of interoperable EHRs[1253]. It has been argued that cross-border data exchange should be "designed with data protection in mind too", meaning that "appropriate measures should be embedded in the network infrastructure

---

1248 *See ibid.*, which follows European Commission, *Annex to the Commission Recommendation on a European Electronic Health Record exchange format*.

1249 *See* e.g. Ed Conley and Matthias Pocs. "GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)". In: *European Journal of Biomedical Informatics* 14.3 (2018), pp. 48–61.

1250 *See* Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 7.

1251 *See* Conley and Pocs, "GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)"; Adeel Anjum et al. "An efficient privacy mechanism for electronic health records". In: *Computers & Security* 72 (2018), pp. 196–211.

1252 *See* Network eHealth. *eHealth Network Guidelines to EU Member States and the European Commission on an interoperable eco-system for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe*. eHealth Network, 2019. The standards will be presented in Chapter 5 Section 5.5.

1253 *See* Conley and Pocs, "GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)".

to secure the access and the data sharing"[1254]. Both the EHR systems and the EU standard formats in the country of origin and in the country of treatment should be designed to "effectively implement the various data protection principles, to guarantee the compliance with the law and to protect the rights of data subjects"[1255]. Open and extendable architecture with DPbD modelling and embedded risk analysis tools provides systematic protection for storage and for the interoperable exchange of personal health data[1256]. As argued in Chapter 2 Section 2.5.3, certification may be used to demonstrate compliance with DPbD and DPbDf obligations, and a one-size-fits-all solution is not available. However, the European EHR Exchange Format of the EC represents a baseline for any EHR implementation.

The implementation of the EC's Recommendation and of the measures outlined above may finally foster the interoperability of EHRs to empower cross-border access to healthcare. Within the EU legal framework, the absence of a uniform and specific legislation on EHRs, and their interoperability, may remain an obstacle for each interoperability layer since progress is the task of the Member States and, as a matter of fact, depends on an update of the state of the art of EHRs. Nonetheless, the EC highly recommended improving cross-border interoperability of EHRs in order to comply with data protection provisions. The GDPR lays down the main requirements that healthcare providers must comply with when using EHRs. Personal health data in EHR systems must also be protected *ex ante* by design and by default. EU policies, methodologies and standards could be a starting point towards productive interoperability.

Then, since the GDPR and its DPbD requirements are applicable in all Member States, a common EU strategy on DPbD for EHRs systems could enhance the "fair and compliant flow of personal health data across EU and therefore, of patients and products"[1257]. This strategy could also lead developers of EHRs to find "clearer and well-defined rules to be followed during systems design"[1258]. Hence, in Chapter 6 a set of guidelines will be presented. Before that, Chapter 5 deals with the technical aspects –

1254 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 7.
1255 *Ibid.*
1256 *See* Abedjan et al., "Data science in healthcare: Benefits, challenges and opportunities".
1257 Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union", p. 7.
1258 *See* for these conclusive considerations *ibid.*

which defines DPbD methodologies, technologies, and standards to be used – and Chapter 4 will provide a comparative analysis with the US legal framework since it sets a specific privacy rule for the healthcare context and EHR systems that requires the implementation of security measures. Before concluding this Chapter on e-health and the case study, the next section follows the final considerations of the previous Chapter on the need to balance the right to data protection with other rights since in this context specific brief considerations may be added to that analysis.

3.5 Balancing the right to data protection against public health

Privacy and data protection are relevant concerns, but at the same time there may be other competing interests at stake. They are not absolute rights. In the context of e-health, the two typical competing interests are on the one hand the right to privacy and data protection of a natural person, and on the other hand, the interest in public health and security. The right to data protection is reconcilable with public health, but safeguards shall be implemented. So, where the data protection right may be restricted to protect the general interest in public health, the least intrusive solutions shall always be preferred in accordance with the requirements of necessity and proportionality. It can be noted that collective health is not an absolute goal capable of legitimising any compression of the individual's rights and freedoms, but it is the "sum" of the protection of each individual's health[1259].

As mentioned, the EU has shared competence with the Member States in specific fields of common safety concerns in public health matters, but the Member State can define its own national health policy and organise healthcare provision, management of health services and allocation of resources[1260]. So, the way to obtain the right balance between competing

1259 *See* ISS Bioethics COVID-19 Working Group. *Data protection in COVID-19 emergency*. Rapporto ISS COVID-19 n. 42/2020, 2020, p. 6.

1260 *See* further on Ionescu-Dima, "Legal challenges regarding telemedicine services in the European Union", p. 109; Di Federico, "Access to Healthcare in the European Union: Are EU Patients (Effectively) Protected Against Discriminatory Practices?"; Kai P. Purnhagen et al. "More Competences than You Knew? The Web of Health Competence for European Union Action in Response to the COVID-19 Outbreak". In: *European Journal of Risk Regulation* (2020), pp. 1–10. Article 168(7) of the TFEU recognises these competences. According to Di Federico, the differences among Member States may create discrimination

interests relies on a concrete case-by-case analysis at the national level[1261]. Member States can set national laws as legal grounds for processing personal health data for substantial public interest, public health interests or medical research interests in accordance with Article 9(2)(g), (i), (j) GDPR, but appropriate and specific safeguards shall always be provided in order to protect the rights and freedoms of the data subjects.

The recent pandemic emergency of COVID-19[1262] has required prompt answers to Member States on how to strike the balance between the rights to privacy and data protection and the public interests of protecting individual or collective health[1263]. Digital technologies were developed to trace individuals, monitor their symptoms or record the contacts of infected people in order to control the movement of population or to enforce confinement measures[1264]. These activities fall under the definition of "processing" of personal data, and the technologies developed during

---

across the EU and impinge on patients' rights. It is of paramount importance to promote equality in healthcare.

1261 This consideration was made even before the GDPR with reference to the DPD, in Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?", p. 87.

1262 The technical name of the infection is SARS-CoV-2. *See* Kristian G. Andersen et al. "The proximal origin of SARS-CoV-2". In: *Nature medicine* 26.4 (2020), pp. 450–452.

1263 *See* CoE Council of Europe. *Digital solutions to fight COVID-19. 2020 Data Protection Report*. Council of Europe. October 2020, 2020; Hannah van Kolfschooten and Anniek de Ruijter. "COVID-19 and privacy in the European Union: A legal perspective on contact tracing". In: *Contemporary Security Policy* (2020), pp. 1–14; Giovanni Comandé, Denise Amram, and Gianclaudio Malgieri. "The democracy of emergency at the time of the coronavirus: the virtues of privacy". In: *Opinio Juris in comparatione. preprint* 1 (2020), pp. 106–121; Oreste Pollicino. "Fighting Covid-19 and Protecting Privacy Under EU Law – A Proposal Looking at the Roots of European Constitutionalism". In: *blog-iacl-aidc.org* (2020). At a comparative level from different perspectives *see* also the Special issue of the journal Diritto Pubblico Comparato ed Europeo – online on "Covid-19 and its constitutional implications" at <www.dpceonline.it/index.php/dpceonline/issue/view/43>. Last accessed 06/10/2021.

1264 *See* the contact tracing solutions collected by the Data Protection Law & Covid-19 Observatory at <lsts.research.vub.be/en/contact-tracing-apps>. Last accessed 06/10/2021. Data Protection Law & Covid-19 Observatory is a collaborative monitoring platform which documented data protection law resources related to the emergency, including soft law and DPA opinions. *See* also the extraordinary measures at the international level described by Joseph A. Cannataci. *Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic*. A/75/147. Special Rapporteur of the Human Rights Council on the right to privacy, 2020.

the emergency impact the right to privacy, the right to data protection of personal data, including personal health data, and other fundamental rights and freedoms, such as dignity, self-determination, democracy, non-discrimination, and freedom of movement.

However, this is not the first time in history. In the past, other serious threats to health required measures for tracing individuals[1265]. In 2020, within the GDPR's framework, Member States' measures were adopted on the basis of Article 9(2)(i) – (j), and Article 23[1266].

Health Threats Decision No 1082/2013/EU provided some definitions which can be still used during the COVID-19 outbreak[1267]. The term "contact tracing" referred to "measures implemented in order to trace persons who have been exposed to a source of a serious cross- border threat to health, and who are in danger of developing or have developed a disease". "Epidemiological surveillance" is processing which implies "the systematic collection, recording, analysis, interpretation and dissemination of data and analysis on communicable diseases and related special health issues". To prevent or control a serious threat to health, a "public health measure" mitigates its impact on public health by collecting a large quantity of personal health data. Any processing of personal data has its purpose,

1265 *See* Patrycja Da˛browska-Kłosin´ska. "Tracing individuals under the EU regime on serious, cross-border health threats: An appraisal of the system of personal data protection". In: *European Journal of Risk Regulation* 8.4 (2017), pp. 700–722; Hannah van Kolfschooten. "EU Coordination of Serious Cross-Border Threats to Health: The Implications for Protection of Informed Consent in National Pandemic Policies". In: *European Journal of Risk Regulation* 10.4 (2019), pp. 635–651, which refers to Ebola; Greer et al., *Everything you always wanted to know about European Union health policies but were afraid to ask*.

1266 *See* the comparative analysis by Giorgio Resta. "La protezione dei dati personali nel diritto dell'emergenza Covid-19". In: *Giustiziacivile.com* (2020). *See* e.g. Dianora Poletti. "Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza". In: *Persona e Mercato* (2 2020), pp. 66–76, which focuses on the Italian situation. Some scholars in the UK even proposed a Bill on Corona-virus safeguards on the basis of the GDPR. *See* Lilian Edwards et al. "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates". In: *LawArXiv, pre-print* (2020). It is worth noting the Data Protection Law & Covid-19 Observatory's classification of law resources. DPAs' opinions are also collected by the IAPP portal at <iapp.org/resources/article/dpa-guidance-on-covid-19/>. It is also worth mentioning the research done by Privacy International organisation at <privacyinternational.org/examples/ tracking-global-response-covid-19>. Last accessed 06/10/2021.

1267 *See* Article 3 of the Decision No 1082/2013/EU.

which can be justified in an emergency health crisis, but it should always be designed to serve humankind[1268].

Therefore, the Joint Statement on Digital Contact Tracing issued by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe claimed that necessary data protection safeguards should be implemented when adopting extraordinary measures to protect public health[1269]. Indeed, several authorities and institutions described appropriate safeguards by creating lists of principles to comply with in the COVID-19 crisis[1270]. On this matter, the previous case law of the ECtHR and the CJEU in the proportionality and security field can also be applied[1271]. The ECtHR indicated that exceptional measures that limit fundamental rights shall be limited in time, be issued according to

1268 Recital 4 GDPR.

1269 *See* Alessandra Pierucci and Jean-Philippe Walter. *Joint Statement on Digital Contact Tracing*. Chair of the Committee of Convention 108 and Data Protection Commissioner of the Council of Europe. Strasbourg, 28 April 2020, 2020.

1270 *See* EDPB European Data Protection Board. *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. European Data Protection Board, 2020; EDPB European Data Protection Board. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. EDPB. 21 April 2020, 2020; EC European Commission. *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. 2020/C 124 I/01), 2020; EC European Commission. *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. L 114/7. 14 April 2020, 2020; Network eHealth. *Interoperability guidelines for approved contact tracing mobile applications in the EU*. eHealth Network. Brussels, Belgium, 13 May 2020, 2020; CNIL Commission Nationale de l'Informatique et des Libertés. *Deliberation N°. 2020–046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid"*. CNIL, 2020; Committee on Bioethics (DH-BIO). *DH-BIO Statement on human rights considerations relevant to the COVID-19 pandemic*. DH-BIO/INF (2020) 2. 14 April 2020, 2020; Group, *Data protection in COVID-19 emergency*; Pierucci and Walter, *Joint Statement on Digital Contact Tracing*.

1271 *See* the interesting analysis by Kolfschooten and Ruijter, "COVID-19 and privacy in the European Union: A legal perspective on contact tracing", which studies the case law on proportionality and security threats to be applied to the Corona-virus outbreak.

1272 Carlo Casonato. "Health at the time of covid-19: tyrannical, denied, unequal health". In: *paper presented at the Conference Biolaw, Globalization and Pandemic. Challenges in the context of COVID-19* (2020), pp. 1–7, p. 2.

the rule of law with a democratic decision-making process, and respect the principle of proportionality after passing a rationality test[1272].

The following legal analysis will use the technical neutrality principle, by avoiding reference to a specific contact-tracing technology or warning method. It will refer to the necessary safeguards for processing personal health data in the emergency health situation that processes a large scale of data in order to protect public and individual health[1273].

First of all, data protection principles of Article 5 of the GDPR shall be guaranteed, but rights and duties can be carefully limited. So, the legal basis should be set by national law in accordance with the GDPR (i.e. lawfulness), and processing should be fair and transparent (i.e. fairness and transparency). The EC has specified that "relying on the law as the legal basis would contribute to legal certainty" since it provides the lawful details of the allowed processing, including the identity of the data controller (i.e. national public health authority)[1274], the processor, the recipients, the specific purpose, and all the safeguards[1275]. The processing settings and privacy policies shall be clear and transparent to data subjects. However, the policies should take into account any limitation to the rights and obligations[1276].

It has also been recommended that open source and open data concepts shall be applied in emergency processing, and the language of the policies

---

1273 According to Plutino, the EU has failed to have a unified approach, but has provided guidelines aimed at inspiring national policies. *See* Marco Plutino. "'Immuni'. Un'*exposure notification* app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici". In: *MediaLaws Rivista di Diritto dei Media* 2 (2020), pp. 172–193, p. 176, which also focuses on the Italian tracking *Immuni*.

1274 The EDPB suggested that national public health authorities could be the data controllers, but other subjects and roles could be identified by law. *See* European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, p. 7.

1275 *See* European Commission, *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. A pan-European approach coordinated at the EU level was recommended by the EC, but the Member States followed different lines of action. So, the present discussion will not refer to a specific legal framework.

1276 Since Article 23 allows a limitation to the rights and obligations established in Articles 12 to 22 and Article 34, some information usually contained in the policies may not be provided. Nevertheless, all the authorities recommended the need to ensure fair and transparent processing to respect the essence of the right to data protection and privacy.

shall be plain to enhance transparency[1277]. Transparency is also a frequent argument for the proportionality test in CJEU case law[1278]. The principle of fairness protects against unforeseeable negative effects, discrimination, and power imbalance[1279]. Thus, the safeguards should prevent stigmatisation while respecting confidentiality, and the measures should be "the least intrusive yet effective"[1280]. In fact, processing should be trustworthy, and the data subjects may choose whether or not to participate in the monitoring programmes voluntarily[1281].

Moreover, the processing of personal health data is allowed insofar as it only serves the purpose of controlling the pandemic crisis (i.e. purpose

1277 *See* point XI of Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 6; European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, pp. 13–14.

1278 *See* e.g. *Digital Rights Ireland* of 2014: Judgement of the Court (Grand Chamber) of 8 April 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof. Joined Cases C-293/12 and C-594/12. On this case *see* Kolfschooten and Ruijter, "COVID-19 and privacy in the European Union: A legal perspective on contact tracing", p. 9.

1279 *See* Chapter 2, Section 2.4.8.

1280 These sentences represent the first and second principles recommended in European Commission, *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*.

1281 *See* point II of Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 4. The voluntary basis has been frequently recommended for avoiding the creation of a widespread and problematic surveillance scenario. On health surveillance, and Orwell's risk *see* the special issue of Rivista n. 158 Formiche. *Orwell 2020. Il virus della sorveglianza*. Rubettino, 2020. ISBN: 9788849863314.

1282 The purpose limitation principle has been stressed by all the authorities. The EDPS pointed out that it is "an essential safeguard to provide individuals with the confidence that the data they provide will not be used against them in an unexpected manner". *See* European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, p. 5. The CoE specified that the purpose shall exclude further processing for commercial or law enforcement purposes. *See* Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, pp. 4–5. On the same opinion *see* European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, p. 7.

limitation)[1282], and is extraordinary and temporary[1283]. The temporary character is actually an argument to be used in the proportionality test in light of the goal of the measure. As a result, the timing of the data storage should be proactively pre-defined taking into account the medical relevance, so personal health data should be kept for no longer than is necessary (i.e. storage limitation)[1284]. Then, they shall be deleted, erased or anonymised when there is no longer a threat to public health[1285].

Data minimisation should govern all processing activities. Personal health data shall be reduced to the strictest minimum[1286]. As explained in the previous Chapter in Section 2.7, the assessment in the "necessity test" will take into account the extent of what is strictly necessary for pursuing the goal of the measure. Personal health data should be limited and, if need, pseudonymised, and then the requirements of DPbD and DPbDf, and the preventive risk assessment (i.e. DPIA) are pivotal and shall be central[1287]. The EC recommended that a list of the personal health data to

1283 *See* Kolfschooten and Ruijter, "COVID-19 and privacy in the European Union: A legal perspective on contact tracing", p. 6; Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 7.

1284 *See* European Commission, *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. In particular, *see* point 3.7. *See* also European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, p. 8.

1285 It should be specified that the data will probably be anonymised for secondary medical research purposes since authorities have the rare opportunity to use a large amount of medical data on a disease. However, it is not clear whether the anonymised health data will be as useful as personal health data. Member States can provide the ground under Article 9(2)(j) GDPR and Article 89 GDPR. On the research field *see* European Data Protection Board, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*; Gianclaudio Malgieri. "Data Protection and Research: A vital challenge in the era of Covid-19 Pandemic". In: *Computer Law & Security Review* (2020); Amram, "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks"; Stuart McLennan, Leo Anthony Celi, and Alena Buyx. "COVID-19: Putting the General Data Protection Regulation to the Test". In: *JMIR Public Health and Surveillance* 6.2 (2020), e19279.

1286 *See* point V of Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 5.

1287 *See* European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, p. 9. The authority highlighted the importance for the DPIA to be publicly available.

be collected should be defined in the legal basis[1288]. The risk to rights and freedoms shall be minimised *ex ante*[1289].

During the processing activities, personal health data should be kept up-to-date and processing should respect the accuracy principle[1290]. Personal health data shall be used adequately, and shall not be disseminated, but shared among involved actors while implementing organisational and technical measures[1291]. Thus, it has been claimed that processing should receive the approval of a national DPA[1292], use appropriate security measures (e.g. encryption, cryptographic techniques), and follow cybersecurity requirements in order to protect availability, integrity, and confidentiality of personal data[1293]. The authorities have drawn attention to the use of a completely automated decision that can affect individuals since data subjects have the right not to be subject to a decision based solely on that kind of processing activity[1294].

Joseph A. Cannataci, Special Rapporteur on the right to privacy for the United Nations, also stressed in his report the importance of the privacy by design approach. *See* Cannataci, *Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic*, p. 15.

1288 *See* European Commission, *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*.

1289 *See* point III of Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 4.

1290 According to the CoE, "as the implications may be serious (self-isolation, testing) for the individuals identified as potential contacts of someone infected, ensuring the quality and accuracy of data is crucial". *See* Pierucci and Walter, *op. cit.*, p. 5.

1291 *See* European Commission, *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. In particular, *see* point 3.5.

1292 In European Commission, *op. cit.*, the EC recommended the involvement of the DPA, but not a formal notification. However, the EC suggested a consultation.

1293 *See* European Commission, *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*; Pierucci and Walter, *Joint Statement on Digital Contact Tracing*; European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*.

1294 As anticipated *infra* in Section 3.3.3, this right usually applies in the healthcare context. *See* European Commission, *Communication for the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*; Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 5.

It should be noted that the final principle of accountability guarantees overall compliance with data protection rules[1295]. Oversight and audits may ensure the respect of these rules. Technologies may be interoperable, so safeguards shall be implemented even in the interoperability scenario[1296]. A more coordinated solution at the EU level would have been a great way of ensuring widespread protection and for better safeguarding democracy and freedoms.

Looking now to the use of EHRs in the COVID-19 situation, some brief considerations can be made. The use of EHRs is useful during a pandemic for connecting organisations and public entities and healthcare providers to check symptoms, monitor treatment outcomes, signal the diagnosis, and collect laboratory results on the tests. Hence, during the pandemic more data may be added to the personal health data collected in the individual's EHR before the health emergency.

Even telemedicine and telecare tools can be very useful in the health emergency since they support authorities "anytime" and "anywhere" during the healthcare provision while preserving safe distances among individuals. The benefit is more effective and widespread disease management than before[1297]. It is clear that this benefit is related both to people infected by Corona-virus and people with other pre-existing diseases who cannot go to hospital for multiple reasons (e.g. during general confinement measures).

Nevertheless, it can also be argued that the use of EHR systems or other e-health technologies in an exceptional processing for public health purposes must be carefully evaluated. EHRs potentially contain all the medical history of the data subject. Therefore, other processing operations that connect the EHR with different e-health technologies or ICTs should

---

The EDPB suggested that the algorithm should be auditable. It pointed out that false positives may occur to a certain degree, but where technically feasible a transparent explanation should be given. *See* European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, p. 8.

1295 *See* point XIII of Pierucci and Walter, *Joint Statement on Digital Contact Tracing*, p. 4.

1296 *See* eHealth, *Interoperability guidelines for approved contact tracing mobile applications in the EU*.

1297 *See* e.g. Francesco Girardi et al. "Improving the Healthcare Effectiveness: The Possible Role of EHR, IoMT and Blockchain". In: *Electronics* 9.6 (2020), pp. 884–900, which analysed the importance of using digital instruments like the EHR or PHR in a health emergency, which can also be bolstered by the use of blockchain or IoT tools.

be prohibited or allowed insofar as restrictive and preventive technical and organisational measures are concretely implemented. The recipients of the personal health data should not be entitled to access all the data in the EHR[1298]. The stigmatisation and discrimination risk level is very high since the Corona-virus is inevitably bound with social exclusion of infected or potentially infected individuals. Even the interoperability policies on EHRs at the EU level should not be used as means for avoiding either the provision of safeguards or the general prohibition on the processing of personal health data[1299].

National laws should provide detailed rules for the use of an EHR in an exceptional processing whose purpose is not solely the provision of individual healthcare, but also the control of a threat to public health. These rules should take into account the DPbD and DPbDf principles, which embed the risk management approach and the need to balance concrete processing characteristics against rights and freedoms.

Protection and regulation by design were discussed in the Second Chapter, where PbD and DPbD were discussed in detail. The present Chapter investigated the e-health care sector and the specific case study for a DPbD implementation. PbD has been recognised as an international principle, and in US federal law there is a specific rule for the implementation of measures in the e-health care context and for EHRs. The protection of personal health data is a global issue, and the technologies are often implemented independently of the physical borders. Therefore, the following Chapter will conduct a comparative analysis between the US HIPAA Privacy Rule in the US legal framework and the DPbD obligation of the GDPR.

1298 A problematic scenario is for example access by the employer to the EHR for work purposes.

1299 On the cross-border exchange of data during the pandemic *see* the Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. C/2020/4934. O.J. L. 227I, 16.7.2020.