D6.6 – Identification of Healthcare Rights to be allocated to the citizen (possibly by design) – first version

Grant Agreement nº:	MSCA ITN EJD n. 814177
Project Acronym:	LAST-JD-RIoE
Project Title:	Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)
Website:	https://www.last-jd-rioe.eu/
Contractual delivery date:	31/03/2021
Actual delivery date:	05/04/2021
Contributing WP	WP6
Dissemination level:	Public
Deliverable leader:	KUL
Contributors:	UNIBO, UAB

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177

Document History

Version	Date	Author	Partner	Description
0.1	06/11/2020	Daniela Brešić	KUL	V1 (preliminary)
0.2	20/12/2020	Daniela Brešić	KUL	V2 (preliminary)
0.3	20/02/2021	Daniela Brešić	KUL	V3 (preliminary)/Internal review (KUL)
1.0	21/03/2021	Daniela Brešić	KUL	V4

Contributors

Partner	Name	Role	Contribution
KUL	Prof. Dr. Anton Vedder	Editor	Review
UNIBO	Prof. Dr. Silvia Zullo	Editor	Review
UAB	Prof. Dr. Pompeu Casanovas	Editor	Review

Table of Contents

List of Acronyms

CJEU	Court of Justice of the European Union
COE Recommendation	Council of Europe recommendation on the protection of health-related data
COE	Council of Europe
DGA	Data Governance Act
EC	European Commission
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eHealth	Electronic Health
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
mHealth	mobile Health
Oviedo Convention	Convention on Human Rights and Biomedicine
OECD	Organisation for Economic Cooperation and Development
UN	United Nations
WHO	World Health Organisation
WP29	The Article 29 Working Party

Executive Summary

This document reports the findings of the deliverable 6.3 “Identification of Healthcare rights to be allocated to the citizen (possibly by design)”. The aim of the deliverable is to provide a preliminary legal and ethical analysis concerning the healthcare rights allocated to citizens and the challenges associated with eHealth technologies that facilitate medical data sharing. The deliverable will introduce the methodology, the state of the art and the critical analysis of the legal and ethical challenges associated with citizens’ healthcare rights. To this end, the deliverable will address the following two issues. First, the deliverable identifies the ethical considerations that need to be taken into account when exploring legal challenges in eHealth and their impact on the citizens’ healthcare rights. Hereto, it applies the widely accepted approach of Principlism taking into account the bioethical principles identified by Beauchamp and Childress. This shall enable to investigate if and to what extend the currently existing confidentiality, privacy, data protection legislations implement the ethical considerations that have been identified. Second, the deliverable identifies and discusses the European legal framework protecting healthcare rights of citizens related to eHealth technologies from the fundamental rights perspective. The relevant fundamental rights laid down in European Convention of Human Rights and the EU Charter of Fundamental Rights will be identified, whereby particular attention will be paid to the fundamental right to privacy, the fundamental right to data protection, and the fundamental right to confidentiality. The analysis will be supplemented by case law set out by the European Court of Human Rights and the European Court of Justice, respectively. Moreover, national confidentiality, privacy, and data protection legislations that codify the citizens’ healthcare rights will be investigated where necessary. In addition, international and European policy documents will be briefly introduced in order to provide an overarching view on the protection of fundamental rights. Finally, the deliverable will present preliminary findings and discuss if the relevant legislations implement the identified ethical considerations sufficiently.

1 Introduction

Taking into account the objectives of the research project, the deliverable will investigate the legal and ethical issues associated with the citizens' healthcare rights in the eHealth sector.

Ethical considerations are fundamental to the protection of citizens' healthcare rights as they provide direction for the protection of individuals according to what is morally desirable. This includes ethical considerations that have already been addressed by the law, but also those beyond it. Various ethical and legal challenges occur through the deployment of eHealth technologies (such as smart watches) and eHealth platforms (such as electronic health records, or research platforms enabling the exchange of health data), as they change the way traditional healthcare is being performed. While the provision of healthcare is traditionally shaped by the doctor-patient relationship, eHealth technologies and platforms lead to an increasing involvement of private technology providers. Furthermore, such tools facilitate the increased involvement of citizens in their respective therapy, as, for instance, smart health devices enable citizens to keep track of their own health status. The possibilities for increased information flow created through the use of eHealth open the door for more efficient healthcare systems and thus raise the question about the ethical implications on citizens.

Primary and secondary legislation entails various rights and safeguards protecting individuals in the eHealth sector. Fundamental rights are the foundation of an individual's rights and freedoms. One important right is enshrined in Article 8 European Convention of Human Rights, which protects the right to respect for private and family life, home and correspondence. The scope of article 8 has been interpreted broadly by the European Court of Human Rights and encompasses the protection of an individual's privacy. The right to privacy therefore plays an important role in guarding the confidentiality of health data, which is considered to be a pivotal principle in the domestic legal systems of the countries subject to the ECHR. However, the resulting guarantee for medical confidentiality is not absolute. For instance, the principle of medical confidentiality may be breached in situations where eHealth becomes relevant, for example, where physicians need to share the citizens' health data with other care providers for the provision of care or for research purposes through digital means such as electronic health records. The trend towards increasing use of eHealth technologies in the healthcare sector makes the protection of the citizens' personal data therefore imperative.

The report thus seeks to provide an analysis of the legal rights allocated to the citizen and the ethical implications of the internet of everything for eHealth. More specifically, it will identify whether relevant ethical consideration that are pertinent to eHealth are sufficiently implemented in the existing privacy, data protection and confidentiality legislations. First, an analysis regarding the ethical aspects relevant to eHealth will be provided, taking into account the four principles of biomedical ethics established by Beauchamp and Childress. Second, the relevant healthcare rights allocated to citizens within the existing privacy, data protection and confidentiality legislations regarding eHealth will be identified. This deliverable thus pursues to explore the citizens' healthcare rights from the perspective of

fundamental rights and the existing, with the aim to critically investigate the legal guarantees of citizens' rights in the healthcare environment. Finally, preliminary results debating the degree of implementation of the identified ethical considerations in existing confidentiality, privacy, and data protection legislations will be provided.

2 Approach

2.1 Problem statement

The European health care system is currently undergoing a transformation towards increased digitalisation through eHealth services, which may include a variety of digital services in healthcare, research, and public health. eHealth tools open new opportunities for citizens to collect and share the data about their health or treatment not only with their physicians but also with other actors such as research institutes or health insurances. Citizens may share their data actively (by making the personal data available themselves) or passively (by letting other stakeholders collect and share the citizens' data) for different purposes, which can benefit other citizens in return through improved public health and the provision of care in general. For instance, the sharing of personal data of citizens can support care providers in better understanding examination results and, subsequently, enable them to provide tailored treatments or personalised medicine in accordance with the personal needs of the patient. Whilst several digital means available on the market facilitate the collection of health data via healthcare applications (e.g. medical devices, telehealth) or platforms (e.g. electronic health records, electronic health cards), a common definition of eHealth services does not exist. Notwithstanding, the use of eHealth services carries with it various legal and ethical implications on citizens and their rights that need to be explored.

2.2 Research questions

This deliverable seeks to answer the following central research question: "Are the principles of biomedical ethics sufficiently embedded in the existing privacy, data protection, and confidentiality legislations when it comes to the protection of citizens' rights in the eHealth sector?".

In order to answer this question, the following sub-questions will be addressed:

1) What do the principles of biomedical ethics in the eHealth environment entail?
   This sub-question will be answered in chapter 3.

2) Which privacy, data protection, and confidentiality legislations protect the rights of citizens at the European, EU and national level and what kind of citizens' rights do the privacy, data protection, and confidentiality legislations grant to citizens when it comes to the sharing of the health data in eHealth?
   This sub-question will be answered in chapter 3.

3) What kind of legal issues arise from the protection of the citizens' healthcare rights that are granted under current privacy, data protection, and confidentiality legislations in eHealth?
This sub-question will be answered in chapter 3 and 4.

4) What kind of ethical issues arise from the protection of the citizens' healthcare rights in eHealth?
This sub-question will be answered in chapter 4.

5) How and to what extent do medical ethics and law (i.e. existing privacy, data protection, and confidentiality legislations) conflict with each other in regards to the protection of the citizens' healthcare rights in eHealth?
This sub-question will be answered in chapter 4.

2.3 Research objective

The research will focus on the investigation of the citizens' rights involved and whether (or in what manners) these rights are being impaired by eHealth technologies and (health) data transfers. Citizens' rights (e.g. the right to access one's data, the right to data portability) might be affected through data transfers, as citizens are not always aware of what kind of data they are transmitting and the fact that data related to their person might not only be stored in their medical file but also in other locations when using healthcare technologies. To this end, the deliverable will focus on the aspects of data protection, privacy, and confidentiality in terms of eHealth tools which facilitate the transfer of citizen-related health data. The deliverable also seeks to offer an interdisciplinary discussion taking into account the legal aspects of citizens' healthcare rights, while also considering ethical considerations by using the principles of biomedical ethics as normative criteria by Beauchamp and Childress.

More specifically stated, the envisaged output of the deliverable includes:

1) A comprehensive overview of healthcare rights of citizens under the current legal framework, i.e. from the perspective of fundamental rights protection as well as data protection, privacy and confidentiality regulation, with a particular view to eHealth;
2) A discussion of currently existing relevant legal (legislative and non-legislative) framework with regard to the protection of the healthcare rights of citizens in the eHealth environment;
3) A discussion of ethical considerations pertinent to eHealth technologies which facilitate the sharing of citizen data;
4) An investigation of ethical and legal impediments with regard to the citizens' healthcare rights and (health) data sharing in eHealth.

2.4 Methodology

2.4.1 Scope and delineation

Due to the interest of the LaST-JD-RIoE research project, the *technological scope* of this deliverable is concerned with eHealth, more specifically with technological health infrastructures which enable the sharing of health-related data. To do so, various ethical sources as well as legal sources (including, in particular, legislations, jurisprudence and literature) will be examined.

The *ethical scope* involves the investigation of ethical considerations that are relevant to eHealth technologies which enable the sharing of health-related data. The principles of biomedical ethics established by Beauchamp and Childress will be applied as the normative criteria. More specifically, the principle of respect for persons and their autonomy, the principle of beneficence, the principle of justice, and the principles of non-maleficence, which may deliver justifications for possible duties and other ethical considerations that may arise in the eHealth context, will be examined. The deliverable seeks to critically assess if and to what extend these ethical considerations have been addressed by the confidentiality, privacy and data protection legislations.

The *legislative scope* involves the examination of the legislative European framework applicable to (health) data sharing and protecting citizens' rights in eHealth. This includes primary law (e.g. the EU Charter of Fundamental Rights) and secondary law. With regard to the latter, the General Data Protection Regulation (EU) 2016/679[1] and the directive on the application of patients' rights in cross-border healthcare[2] play are of importance, as the General Data Protection Regulation aims to protect data subjects in terms of the processing of their sensitive health data, while the directive on patient's rights protects individuals in cross-border healthcare. Also, non-legislative acts will be examined, whereby attention will be given to the recommendation of the Council of Europe on the protection of health-related data[3] as it provides guidelines, as soft-law, on the sharing of health-related data through digital means. These instruments therefore play an important role for the protection of citizens and their rights in terms of (health) data sharing in the eHealth environment. Furthermore, national legislations with regard to relevant legal issues regarding the sharing of (health) data and eHealth platforms will be examined.

The choice of *national jurisdiction* is influenced by the language proficiency and will take into account German- and English-speaking countries. National legislations that are relevant

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Hereinafter 'GDPR').

[2] 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.
OJ L 88, 4.4.2011, p. 45–65

[3] Council of Europe (2019) Recommendation CM/Rec(2019)2 of the Committee of Ministers to Member States on the protection of health-related data, adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies (Hereinafter 'CoE recommendation').

to the sharing of health data and eHealth platforms will be investigated. It will take into account the national legislations of EU Member States, namely Germany, Austria, and Ireland. These countries have established relevant legal frameworks with regard to the processing of health data and/or concrete eHealth legislations. Given the relevance of the Council of Europe recommendation, the deliverable will investigate the national legislation in the United Kingdom. Since the GDPR is not applicable anymore after the completion of the transition phase in 2020, it could be worth following possible changes and their implications on the processing of health data.

2.4.2 Research structure and methodology

To achieve the objectives of the research, the deliverable will consist of a number of components aiming at identifying the legal and ethical issues associated with citizens' healthcare rights in the context of eHealth. More specifically, it will discuss the issues at stake in relation to the eHealth technologies which facilitate the sharing of personal data between different stakeholders. This deliverable will therefore focus on the citizens' rights in healthcare and may refer to the rights of other stakeholders involved in eHealth (e.g. researchers and physicians) insofar as they become relevant to the protection of the citizens' healthcare rights.

2.4.2.1 Analysis of the ethical values related to the citizens' healthcare rights

As a first step, it is necessary to set the context of the deliverable as a pre-condition in order to enable an interdisciplinary analysis concerning the citizens' healthcare rights within the eHealth environment. This section aims to examine the citizens' rights and principles protecting citizens in the healthcare setting. It will critically assess what aspects could or should be considered when elaborating on citizens' healthcare rights in eHealth. More specifically, it will introduce the widely accepted principles of biomedical ethics by Beauchamp and Childress as normative criteria for the ethical analysis. These principles will build the basis for exploring relevant ethical values in eHealth, namely the principle of respect of persons and autonomy, the principle of beneficence, the principle of non-maleficence, and the principle of justice. This section is based on a normative-evaluative approach. The analysis conducted during the first phase of the research shall enable to refine the approach envisaged for the following phases.

2.4.2.2 Descriptive mapping of the citizens' healthcare rights legislations at the international, European, EU and national level

In a second step, the deliverable will define the context of the research in terms of legislation covering citizens' and patients' healthcare rights in relation to eHealth on an international, European, and (where relevant) national level. Consideration will be given to the legislative framework of the European Union, in particular the General Data Protection Regulation, and the Directive on patient's right in cross-border healthcare. Domestic law will be taken into account insofar as specifications of relevant legal concepts are subject to national competences, and which ought facilitate a comparative examination of national approaches.

Moreover, the deliverable intends to also evaluate existing non-legislative instruments such as the Council of Europe Recommendation on the protection of health-related data, as it provides guidance on the processing of health-related data. Furthermore, the explanatory guidelines by the Article 29 Working Party (now EDPB), the OECD and possibly other institutions will blend into the analysis. This phase is based on a descriptive-explanatory approach.

2.4.2.3 Analysis of the legal issues related to the citizens' healthcare rights

Furthermore, the deliverable entails an examination of the existing framework will as regards to how and to what degree the legislative framework could restrict the exercise of the citizens' healthcare rights in the eHealth sector. It will investigate the legal issues related to citizens' healthcare rights and will, thus, critically assess what aspects should be considered when elaborating on obstacles occurring in the eHealth environment. This analysis takes into account an important rationale of the existing data protection legislation, which puts data subjects into the centre of protection. The investigation of the legal state of the art will facilitate the ethical investigation, aiming at exploring if and to what extend the current confidentiality, privacy, and data protection legislations sufficiently implements the ethical considerations relevant in the eHealth sector. The second phase is based on a evaluative-comparative approach. For this section mainly literature study and legal analysis will be used.

2.4.2.4 Analysis of the impediment between ethics and law related to the citizens' healthcare rights

The previous assessment will feed into the final task and enable the elaboration on the impediments between the law and ethics. The report will deliver preliminary results in terms of the examination of various ethical issues accompanying the legal investigation conducted. In particular, this section will explore the ethical implications for citizens in terms of eHealth tools which enable medical data sharing and the processing of health data in general. It will apply the bioethical principles by Beauchamp and Childress, i.e. the principle of respect for persons and autonomy, the principle of justice, the principle of non-maleficence, the principle of beneficence. The deliverable will analyse ethical issues on the basis of literature study. This section is based on a normative-evaluative approach.

3 State of the art

3.1 Introduction

The provision of adequate healthcare in Europe is being challenged by increased life expectancy, the rise of chronic diseases and demographic transitions.[4] In order to maintain high quality healthcare, the European Commission suggests that healthcare systems need to address these obstacles by strengthening the prevention of illnesses and the promotion of health by shifting healthcare towards primary care instead of hospital care. To support this shift, the European Healthcare System is changing towards digitalisation as the use of new technologies in healthcare provides numerous benefits to patients, care providers, the national healthcare systems and society overall. The improvement and efficiency of healthcare, medical research and public health depend upon the access to relevant patient data and therefore also the exchange of (health) data.

eHealth services, more specifically, encompass various digital services in healthcare, research and public health, offer new possibilities for transforming the healthcare system.[5] The term eHealth generally describes the use of information and communication technologies in the healthcare sector in order to address health issues based on the obtained information.[6] However, there is, as of yet, no commonly accepted definition of "eHealth".[7]

The citizens' data can be collected through various tools, such as wearables (e.g. smart phones), specific healthcare applications (e.g. medical devices, telehealth) or eHealth platforms (e.g. electronic health records).[8] eHealth technologies and platforms may store or facilitate the transfer of different kinds of personal data such citizens' master data (e.g. name, diagnosis, insurance information), emergency data (e.g. information about the citizens' blood type), medication plans et cetera. However, it may not always be evident what type of data constitutes data concerning health[9]. For instance, some technologies collect administrative data (e.g. address, location), which, at a first glance, does not constitute health data but is being processed in the medical context. Moreover, data concerning health collected in a

[4] European Commission (2018) Commission staff working document on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society COM(2018) 233 final, p. 2.

[5] European Commission (2018) Commission staff working document on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society COM(2018) 233 final, p.2-3.

[6] Council of Europe (2015) Introductory report for updating recommendation R(97) 5 of the council of Europe on the protection of medical data by Jeanne Bossi Malafosse. T-PD(2015)07. 3; Norman CD, Skinner HA (2009) eHealth Literacy: Essential Skills for Consumer Health in a Networked World. Journal of medical Internet research vol. 8,2 e9. Doi:10.2196/jmir.8.2.e9.

[7] Boogerd EA et al (2015) "What Is eHealth": Time for an update?. JMIR Res Protoc 2015;4(1):e29.

[8] Riazul Islam SM et al (2015) The Internet of Things for Health Care: A Comprehensive Survey 3 IEEE Access 678.

[9] Data concerning health is defined as "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", article 4(15), recital 35 GDPR.

professional medical context (e.g. for the citizens' treatment, healthcare, or epidemiological research etcetera) has also been referred to as medical data forming part of the broader concept of data concerning health.[10]

However, the (re-)use of health data has the potential to support, inter alia, the quality of care, medical research, patient safety, and public health. eHealth technologies that facilitate the sharing of health data can facilitate the use of personal data, but must respect the fundamental rights of citizens and individuals at all time. Even so, eHealth tools raise new ethical challenges and questions that may need to be considered within the ethical-legal debate. The goal of this deliverable therefore is to explore if and to what extent ethics have been taken into account when promoting the sharing of health-related data of citizens in eHealth.

3.2 Analysis of the ethical implications of IoE for eHealth

The following section will analyse the ethical implications that are relevant to the protection of citizens' healthcare rights in eHealth. In a first step, it will elaborate on the importance of ethics for the legal debate by exploring the relationship between law and ethics. In a second step, the section will explore the ethical values that need to be considered when it comes the use of eHealth technologies in healthcare, namely those values from within the existing confidentiality, privacy, and data protection legislations as well as those beyond them. This analysis will form the basis for the investigation on whether relevant ethical values have been taken into account by the above-mentioned legislations, and, if so, to which degree.

3.2.1 The relationship between law and ethics in general

Confidentiality, privacy, and data protection are fundamental human rights enshrined in the EU Charter of Fundamental Rights at EU level and the European Convention on Human Rights at European level. In particular the concept of data protection seeks to protect citizens from the unlawful use of their personal data. Data protection is therefore intrinsically connected to the ethical values of autonomy and human dignity.[11] Although ethical values often build the foundation for the law, the law primarily offers a regulatory framework where various parties can process personal data in accordance with the established rules. Legislation itself, however, does not provide for the necessary means to address all morally unsought outcomes, as some processing activities, that are lawful, may not always be ethical. Ethics is an important means to add value to legal debates in terms of the desired ethical usage of data by data controllers and data processors, the management of harmful risks, or even the development and deployment of digital technologies. It therefore offers a basis for the law

[10] Mulder T (2019) The Protection of Data Concerning Health in Europe. 5 European Data Protection Law Review 209; The Article 29 Working Party (2015) ANNEX 'health data in apps and devices' to the letter of the WP29 to the European Commission on the clarification of the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[11] European Commission (2018) Ethics and data protection. 14 November 2018, p. 1. Available here: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf

but also a normative source for the interpretation of the law and guidance in addition to what the law demands.[12] Given the risks that the use of special categories of data (formerly referred to as "sensitive data") of citizens poses to the fundamental rights and freedoms of citizens, ethical considerations are essential when processing health data. This is why this type of personal data requires higher protection. However, although confidentiality, privacy and data protection legislations are driven by ethical values, these legislations may have an adverse effect on ethics insofar as they impede other moral values or duties that are important to the sharing of health data. For instance, in medicine, the physicians' duty of confidentiality constitutes an important ethical value which, at first glance, stands in contradiction to the sharing of citizen data. The following section will therefore investigate relevant ethical values in eHealth with the goal of identifying potential impediments between ethics and the law in terms of the application of eHealth tools.

3.2.2 The principles of biomedical ethics

In the medical context, the four bioethical principles established by Beauchamp and Childress are widely accepted The following section will therefore apply the concept of *Principlism,* which considers four moral values, namely the respect for persons and autonomy (1), the principle of justice (2), the principle of non-maleficence (3), and the principle of beneficence (4).[13] Although these principles are not legally binding, they are widely acknowledged to provide orientation for the protection of citizens in the eHealth context.[14]

3.2.2.1 Respect for persons and autonomy

The principle of respect for persons and autonomy protects the fundamental right to self-determination. The term "autonomy" traditionally encompassed various connotations such as self-governance or a person's freedom of the will but is, yet, not necessarily "excessively individualistic" in the sense that the need for individual choices prevails other people's desires or rights.[15] The principles of respect for persons and autonomy in general integrates two aspects: the first one is the liberty to make autonomous choices as an agent, the second is protection of autonomy when it is weakened. When exploring this ethical principle in eHealth and eHealth services, it becomes apparent that citizens are becoming increasingly engaged in their own treatment. Even though the technical implementation is still in development, the successful transformation towards an eHealth eco-system and the provision

[12] Verhenneman G, Vedder A, WITDOM, Legal and Ethical framework and privacy and security principles. Deliverable 6.1, p. 7, 40. Available here: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6%201_Legal%20and%20EthicalFrameworkand%20Privacy%20and%20Security%20Principles_v1.0_final_20150630.pdf

[13] Beauchamp TL, Childress JF (1979) Principles of Biomedical Ethics, Oxford University Press.

[14] Verhenneman G, Vedder A, WITDOM, Legal and Ethical framework and privacy and security principles. Deliverable 6.1. Available here: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6%201_Legal%20and%20EthicalFrameworkand%20Privacy%20and%20Security%20Principles_v1.0_final_20150630.pdf

[15] Beauchamp TL, Childress JF (1979) Principles of Biomedical Ethics, Oxford University Press, p. 57-58.

of better health care services rely heavily on the data output and input provided by the patient.[16] eHealth services therefore have the potential to enhance the participation of citizens in their own healthcare, which can have the effect to support individuals in their autonomous decision-making, other citizens and the care system overall. Despite the benefits that eHealth can bring to citizens, there is a possibility that the human aspects can get lost within their application and that individuals may become a means to an end without the capability to impact on the deployment of eHealth technologies, thereby adversely affecting the person's dignity.[17] To avoid this, stakeholders involved (e.g. physicians, researchers) should ensure that citizens are adequately informed about the use of their data as well as potential risks accompanying such use.

3.2.2.2 Principle of justice

The principle of justice requires to treat persons based on fairness and in respect of their individual vulnerabilities. This entails that individuals should be treated equally when equal but unequally where their needs differ. A commonly accepted aspect of the justice principle is non-discrimination, which forbids to treat individuals differently without cause based on unaccepted considerations.[18] Whereas the principle of beneficence looks, in general, at the overall benefits, the principles of justice takes into account the adequate distribution of justice.[19] Justice therefore may require to have a particular look at the welfare of vulnerable people instead of overarching societal interests. The principle of justice may favour the use of eHealth means to support the prevention and control of rare diseases.

3.2.2.3 Principle of beneficence

The principle of beneficence obliges to increase potential benefits by advancing the good of ethical and fundamental values to the benefit of others. This means that citizens' health data should be used in a way that maximises the welfare of other citizens within the society, while respecting and protecting the rights of others. Beneficence therefore necessitates more than just refraining from harming others, because it requires to actively contribute to benevolent outcomes. eHealth tools have the potential to benefit others, as it facilitates to collect and share valuable information about one's health, which could be used in research or to enable public health protection. In eHealth, the principle of beneficence could therefore require

[16] DIGITALEUROPE (2020) Harnessing the power of AI in health applications – How EU policies can foster the development of an ethical and trustworthy AI to bring better health to citizens, 14.01.2020, p. 18. Available here: https://www.digitaleurope.org/resources/harnessing-the-power-of-ai-in-health-applications/

[17] Faiella G et al, Building an Ethical Framework for cross-border applications: the KONFIDO project, p. 5. Available here: https://konfido-project.eu/sites/default/files/publications/5faiellaethicalframework.pdf

[18] Verhenneman G, Vedder A, WITDOM, Legal and Ethical framework and privacy and security principles. Deliverable 6.1, p. 40. Available here: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6%201_Legal%20and%20EthicalFrameworkand%20Privacy%20and%20Security%20Principles_v1.0_final_20150630.pdf

[19] Beauchamp TL, Childress JF (1979) Principles of Biomedical Ethics, Oxford University Press, p. 213.

citizens to use eHealth technologies. Considering that the usage of electronic health records is voluntary in some countries, the principle of beneficence could argue in favour of an ethical duty of citizens to use eHealth technologies. Furthermore, the sharing of health data through eHealth technologies has the potential to serve wider goals for the benefit of the society. Sharing eHealth data therefore can be benevolent to other citizens. Against this backdrop, the principle of beneficence is not infinite and finds its limits where the individuals' contribution to welfare causes disproportionate harm to themselves. Nonetheless, a duty to benefit others may also require to take into account the utility with the aim to weigh the envisaged good against potential drawbacks. The principle of beneficence may override the principle of non-maleficence where a major benefit causes minor harm.[20]

3.2.2.4 Principle of non-maleficence

The principle of non-maleficence is connected to the physicians' Hippocratic Oath "Above all [or first] do not harm" and obliges to abstain from causing harm or creating risks of harm to others insofar, as it is in one's control not to do so. Against this backdrop, in the eHealth context, this principle may primarily oblige persons who process citizens' data (e.g. physicians, researchers, platform operators and other stakeholders involved in eHealth) to refrain from the harmful use of the personal data of citizens. Unauthorised access and use of sensitive health data of citizens therefore should be avoided, as it violates this principle. Nonetheless, this principle might entail obligations for citizens as well. eHealth platforms do not only store data about one's individual health, but may also contain information about family members or other persons. Individuals therefore may be required to refrain from sharing information about other individuals in order to avoid risks or a negative impact on the other individuals' rights and safety. It could be argued that the principle of non-maleficence therefore may require to respect the confidentiality of other citizens' personal data and their rights and freedoms.

3.3 Citizens' healthcare rights

Chapter 3.3 will present various legal frameworks that aim to protect the fundamental rights and values of privacy, confidentiality, and data protection to the benefit of the citizen at European, EU, and national level. The most important examples include the European Convention of Human Rights, the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation, and the national codes of medical profession. Additionally, international and European policy documents will be explored with the aim of identifying the citizens' healthcare rights in eHealth.

3.3.1 Introduction

The Treaty of Maastricht has assigned an important role to the EU when it comes to the protection against major health threats, which was further emphasized in the Treaty of

[20] Beauchamp TL, Childress JF (1979) Principles of Biomedical Ethics, Oxford University Press, p. 168.

Lisbon, amending the Treaty on European Union and the Treaty on the Functioning of the European Union, and which has strengthened the relevance of public health policy. While the competence for healthcare remains a primarily national matter, the EU's engagement still is pivotal for further improvement of public health and healthcare systems. Article 168 in conjunction with Article 114 TFEU serves as a legal basis for the integration of EU health policies, fostering amongst other things the prevention of diseases, the protection and response to health threats (e.g. epidemics, pandemics) and the harmonization of national healthcare systems.[21] eHealth technologies, in particular, serve the improvement of health-related issues and form part of the EU's strategy to promote personalized care and empower citizens.[22]

The rapid growth of eHealth technologies and their capabilities to exchange data prompt the need for protecting citizens' rights. Individual citizens' rights are not yet explicitly embedded as fundamental rights in the European legislation, but nonetheless enjoy protection under various rights enshrined in the ECHR and the EU Charter.[23] All European Union Member States, in principle, have allocated a number of rights to citizens but transpose them in different ways: while some have implemented citizens' rights into concrete, codified legislation, others have established charters (e.g. citizens' rights charters, charters of services), representatives (e.g. ombudsmen) or even mechanisms for dispute resolution.[24]

Member States are obliged to sustain the protection of citizens' rights by observing their proper transposition and monitoring possible breaches.[25] However, this process and resulting from that, the citizens' rights, are being challenged by the vast technological advancements in eHealth. The following section will, thus, entail an investigation of the fundamental rights of citizens and map the legal landscape regarding healthcare rights of citizens at the international, the European, the EU as well as at the national level. Whilst acknowledging that the definition of rights may assume responsibilities for both citizens and healthcare providers in doing so[26], it aims to analyse the state of the art in terms of the current protection of the citizens' healthcare rights in eHealth.

[21] European Parliament, Public Health – Fact Sheets on the European Union - 2021. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/49/public-health

[22] The EU started multiple initiatives to enhance digital care. See, for instance: Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society (COM(2018) 233), or the Communication on a Digital Single Market strategy (COM(2015) 192).

[23] For instance, the right to respect for private and family life grants protection to citizens under Article 7 EU Charter, which correspond in accordance with Article 52(3) EU Charter to the rights guaranteed by Article 8 ECHR.

[24] European Charter of Patients' Rights, Basis Document, Rome, November 2002, p. 1. https://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf

[25] European Court of Human Rights (2015) "Health-related issues in the case-law of the European Court of Human Rights", Thematic Report, p. 6.

[26] European Charter of Patients' Rights, Basis Document, Rome, November 2002, p. 3. https://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf

3.3.2 Fundamental rights

3.3.2.1 Right to privacy

3.3.2.1.1 European Convention on Human Rights, Article 8

At the European level, Article 8 ECHR protects the right to have one's private life respected and guarantees individuals a sphere without interference from public institutions as a fundamental human right. The European Convention on Human Rights constitutes a legal instrument whose main objective is to impose *negative obligations* on *states* to protect individuals against arbitrary interference with the exercise of fundamental rights [27]. Additionally, Article 8 ECHR entails positive obligations holding Member States accountable for interferences with the human rights due to an omission or lack of action. It requires Member States to ensure that the rights enshrined in Article 8 are upheld between private parties as well.[28] The European Court of Human Rights clarified in its case-law that, in order to evaluate if such a *positive obligations* exists, a fair balance has to be undertaken "between the general interest of the community and the competing interests of the individual concerned, the aims in the second paragraph of Article 8 being of a certain relevance".[29] This subsequently obligates private and public entities in the eHealth sector to ensure that the right to respect for private and family lives can be guaranteed when providing eHealth services.

The *notion of "private life"* has been shaped by the jurisprudence of the European Court of Human Rights. The court repeatedly held this broad term to be incapable of an exhaustive definition and going as far as including interactions with other people taking place in a public environment.[30] The broad notion for the respect for one's private life, which generally encompasses professional or business activities as well, has been said to be in harmony with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which defines personal data as "any information relating to an identified or identifiable individual".[31] The European Court of Human Rights held moreover that information about an individual's health deserves protection under the right to private and family life as such information forms an essential part of it.[32] In the case of *Z. v. Finland*, the court emphasised the importance of respecting the confidentiality of health data as a vital

[27] ECtHR, Case of Kroon and Others v. the Netherlands, Judgment (Application no. 18535/91), 27.10.1997, para. 31.
[28] ECtHR, Case of Bărbulescu v. Romania, Judgement (Application no. 61496/08), 05.09.2017, para. 108-111. Case of Evans v. the United Kingdom, Judgement (Application no. 6339/05), para. 75.
[29] Case of K.H. and Others v. Slovakia , Judgment (Application no. 32881/04), 06.11.2009, para. 45; see also Case of Gaskin v. the United Kingdom, 07.07.1989, Series A no. 160, para. 42.; For instance, the ECtHR confirmed in the Case of Roche v. the United Kingdom the occurrence of a positive obligation where individuals requested access to information about risks to their health threatened through the engagement in army gas tests; see Case of Roche v. the United Kingdom, Judgement, (Application no. 32555/96), 19.10.2005.
[30] ECtHR, Case of Peck v. the United Kingdom, Judgment, Application no. 44647/98, 28.04.2003, para. 57.
[31] Case of Rotaru v. Romania, Judgement (Application no. 28341/95), 04.05.2000, para. 43-44; see also Case of Amann v. Switzerland, Judgement (Application no. 27798/95), 16.02.2000, para. 65.
[32] ECtHR, Case of Z. v. Finland, Judgement (Application no. 22009/93), 25.02.1997.

principle in domestic legislation. This principle has a two-folded objective, taking into account the protection of the individual when receiving healthcare on one hand and the healthcare system overall on the other. It pursues to preserve the patients' individual privacy while at the same time maintaining their trust in medical professionals and in health services overall. The absence of such protection may incite individuals to evade medical assistance, thereby risking to expose themselves and others to health threats. The European Court of Human Rights thus highlighted the need for implementation of appropriate safeguards in national legislation with the aim to prevent the disclosure of the individual's health data.[33]

In accordance with Article 8 ECHR, an *interference* with the right to private and family life occurs where information about an individuals related to his or her private life is stored by a public authority.[34] Notably, the European Court of Human Rights issued that the disclosure of medical records containing sensitive information about the patient constitutes an interference with the right to respect for private life. In the case at stake, the clinic disclosed personal information related to an abortion to a group of public servants without the consent of the patient.[35] Article 8 (2) ECHR stipulates the conditions for the necessity test which may *justify* an interference with the rights enshrined in Article 8 (1) ECHR. In particular, paragraph 2 explains that the interference by a public authority may be justified if three requirements are cumulatively fulfilled, namely if the justification is in accordance with the law (1), in any of the interests enumerated in Article 8 (2) ECHR (2), and necessary in a democratic society (3). It therefore requires that the interference with the right to respect for private life must be proportionate to the legitimate aim. According to paragraph 2, a legitimate aim may be the interest of national security, public safety or the economic well-being of the 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.

3.3.2.1.2 Charter of Fundamental Rights of the European Union, Article 7

Under EU law, Article 7 EU Charter guarantees the identical right to respect for privacy as article 8 ECHR, and imposes negative and positive obligations upon public institutions of the EU and EU Member States.[36] Fundamental rights enshrined in the ECHR and EU Charter obligate the state, but may create a horizontal direct effect in private relationships.[37]

3.3.2.1.3 Citizens' healthcare rights at national level

The following section will briefly introduce the patient's rights introduced on the national level in the countries of Germany, Austria, Ireland and the UK. Every country covers different aspects related to the citizens' fundamental rights protection, such as the citizens' treatment

[33] ECtHR, Case of Z. v. Finland, Judgement (Application no. 22009/93), 25.02.1997, para. 95.
[34] ECtHR, Case of Rotaru v. Romania, Judgement (Application no. 28341/95), 04.05.2000, para. 43-44; Case of Amann v. Switzerland, Judgement (Application no. 27798/95), 16.02.2000, para. 65.
[35] ECtHR, Case of M.S. v. Sweden, Judgement (Application no. 74/1996/693/885). para. 35.
[36] Choudhry S (2014) Right to Respect for Private and Family Life (Family Life Aspects). In Peers S, Hervey T, Kenner J, Ward A (eds.). *The EU Charter of Fundamental Rights: A Commentary* (pp. 183-222) London: Hart Publishing, article 7, para 0718B, p. 201.
[37] Article 52 EU Charter.

and care, research, damage compensation et cetera. The following section therefore seeks to provide a general overview on how the citizens' rights are nationally implemented. Given the focus of the deliverable on the citizens' rights in eHealth, noteworthy aspects integrated in the national confidentiality, privacy, and data protection legislations will be introduced briefly where deemed relevant.

3.3.2.1.3.1 Germany

While some fundamental rights protecting patients are explicitly mentioned in the German basic law, patients' fundamental rights have traditionally been evolving from jurisprudence. For instance, the German Federal Constitutional Court granted patients the entitlement to documentation and to inspection of medical files based on the right to self-determination which derives from the general right of personality[38].[39] Similarly, the fundamental right to data protection derives from the fundamental right to self-determination. In 2013, the German legislator implemented the Patients' Rights Act (*Patientenrechtegesetz*)[40], which introduces new provisions in the German Civil Code and amends the Social Insurance Code 5 (*Sozialgesetzbuch V*). The amending law reinforced, inter alia, the integration of a specific treatment contract between care providers and patient, information duties towards patients, the right to access patient files and the right to receive a paper or electronic copy of the patient file[41] The rules of the GDPR now apply in addition since its introduction. Furthermore, the Patient Data Protection Act (*Patientendaten-Schutz-Gesetz*)[42] as amending law has been introduced in 2020, which regulates inter alia the possibility to have patient data transferred to a electronic patient file from 2022 onwards, to send ePrescriptions via app, and to donate data for scientific research as of 2023. Notably, the use of the electronic patient file is voluntary and the patient will have the possibility to determine to what kind of information the physician should have access.

3.3.2.1.3.2 Austria

In Austria, the rights of patients are summarized in the patient charter, which situates amongst other things the right to treatment, the right to respect for human dignity, right to self-determination, and the right to information and documentation. The patient charter is an agreement as per article 15a Federal Constitutional Law (*Bundes-Verfassungsgesetz)* concluded between the federation and each of the regional provinces. This agreement obliges to safeguard the patients' rights, which are codified within several legislations at federal and regional level (e.g. Austrian General Civil law, Austrian Criminal Code). Notably, the right to data protection is explicitly enshrined as a fundamental right in Article 1 of the Austrian Data Protection Act, which shall protect "the right to secrecy of the personal data concerning

[38] Article 2(1) in conjunction with Article 1(1) German Basic Law.
[39] Di Fabio U in: Maunz, Theodor/ Dürig, Günter (2001) Grundgesetz Kommentar, Verlag C.H. Beck Müchen, Art. 2 Abs. 1, para. 139.
[40] Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten, 20.02.2013, BSGBl. 2019 I Nr. 9.
[41] Section 630c, 630g German Civil Code.
[42] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastructure (Patientendaten-Schutz-Gesetz-PDSG), 19.10.2020, BSGBl. 2020 I Nr. 46, p. 2115.

that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection". It is worthwhile to mention that paragraph 2 further stipulates that restrictions to the right to secrecy are only allowed for reasons of overriding legitimate interests if the personal data is not used in the vital interest of persons or their consent. To this end, the fundamental right to data protection integrates two important notions to the protection of personal data, i.e. consent and secrecy.

3.3.2.1.3.3 Ireland

Several fundamental rights which protect patients are not specifically codified in the Irish constitution and have been evolving from case law (e.g. the right to privacy, and the right to self-determination)[43]. For instance, the fundamental right to privacy and the right to bodily integrity are implied rights in the Irish Constitution deriving from Article 40.3 Irish Constitution which sets out personal rights. The right to data protection is codified as a statutory right in the Irish Data Protection Act. Patients' rights in general are integrated in various Irish legislations at the national level, such as the Health Act or the Medical Practitioners Act. However, the Ombudsman's Statement of Good Practice for the Public Health Service in Dealing with Patients addresses the patients' rights more specifically. This non-binding code of good practice enumerates, for instance, various human rights and values relevant in the healthcare sector. Notably, with regard to the processing of patient data, the code suggests that the protection of identifiable patient data "must be appropriate to the manner of their storage".[44]

3.3.2.1.3.4 The United Kingdom

In the United Kingdom, several patients' rights are implicitly protected by the national Constitution. Patient rights are set out in the NHS Constitution for England[45] which is accompanied by a handbook and which applies specifically to England. The NHS Constitution for England establishes a set of values and principles pertinent to healthcare. It introduces principles that guide the national healthcare system when it comes to patients' rights and responsibilities, as well as the rights and responsibilities of the staff working for the NHS. The document refers to the right to receive information about test and treatment options, the right to access health records, and, notably, to have inaccurate information stored in health records corrected. Also, the NHS Constitution for England provides several pledges in regard to the processing of data. Amongst other things, the NHS pledges to keep confidential data safe and secure, to anonymise patient data in the course of the patients'

[43] European Commission (2016) Patients' Rights in the European Union Mapping eXercise. Final Report, p. 70. Available here: https://ec.europa.eu/health/sites/health/files/cross_border_care/docs/2018_mapping_patientsrights_frep_en.pdf

[44] Ombudsman (2012) The Ombudsmans Statement of Good Practice for the Public Health Service in Dealing with Patients. Available here: https://www.ombudsman.ie/publications/reports/a-report-by-the-ombudsman/

[45] Department of Health & Social Care (2021) The NHS Constitution for England. Available here: https://www.gov.uk/government/publications/the-nhs-constitution-for-england

treatment and to process it for research purposes and the improvement of care for others, and to allow the patient to object if identifiable data has to be processed.

3.3.2.2 Right to protection of personal data

3.3.2.2.1 Article 8 ECHR and Convention 108/108+

Even though not explicitly mentioned in the wording of the European Convention on Human Rights, the right to data protection has been recognized in the case law by the European Court on Human Rights under the right to respect for private life protected by Article 8 ECHR. This was enabled through the broad interpretation of the term "private life" which helped to adapt to the constantly changing technological evolutions. However, the fundamental right to privacy and the fundamental right to data protection are two distinct rights. This difference becomes apparent when comparing the scope of application of both fundamental rights. The concept of data protection is broader than the concept of privacy under the European Convention on Human Rights, as not all information related to an identified or identifiable person are subject to protection under the right to privacy as set out in the European Convention on Human Rights.[46] In particular, the definition of personal data leads to the extension of the scope of the right to data protection.[47] This means that even public personal data can fall under the scope of the right to data protection. The definition of personal data however has been shaped by an important international instrument: the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108[48]). The data protection Convention issued by the Council of Europe is legally binding for its contractual parties and also includes states that are not necessarily subject to the ECHR. The modernization of the Convention 108 (Convention 108+[49]) has strengthened the protection of personal data by, inter alia, integrating data protection principles (e.g. transparency, data minimization) into the updated instrument. Also the ECtHR emphasized the need for data protection principles. For instance, the ECtHR affirmed in the case of *L.H. v. Latvia* that the processing of sensitive data concerning a person constitutes an interference with the right to respect for private life.[50] Subsequently, the transfer of medical data by a hospital to a public authority violated Article 8 ECHR, as the public authority failed to assess in advance whether the collection of the applicant's medical data was '"potentially decisive", "relevant" or "of importance"'.[51]

[46] Biasin E, Brešić D, Kamenjašević E, Notermans P, SAFECARE. Analysis of ethics, privacy, and confidentiality constraints, Deliverable 3.9, p. 13. Available here: https://www.safecare-project.eu/wp-content/uploads/2020/02/Analysis-of-Ethics-Privacy-and-Confidentiality-Restraints.pdf

[47] Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law. Vol. 3. No. 4, p. 225.

[48] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 28/01/1981 - Treaty open for signature by the member States and for accession by non-member States.

[49] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

[50] Case of L.H. v. Latvia, Judgment (Application no. 52019/07), 29.07.2014, para. 33.

[51] Case of L.H. v. Latvia, Judgment (Application no. 52019/07), 29.07.2014, para 58.; see also: Case of M.S.

3.3.2.2.2 Article 8 EU Charter

In contrast to Article 8 ECHR, Article 8 Charter of Fundamental Rights of the European Union (EU Charter) specifically guarantees the right to protection of personal data and follows a concrete aim, namely to protect the processing of personal data through both private and public entities. Article 8 EU Charter therefore protects the personal data concerning an individual and, furthermore, grants the right of access to personal data collected concerning a persona as well as the right to have it rectified according to article 8(2) EU Charter. The EU Charter is legally binding as per Article 6(1) TFEU, while the essence of the right as per Article 51(1) EU Charter has been said to yet not be ascertain.[52] As the Charter of Fundamental rights became legally binding, the right to data protection found its way into the EU Treaties where it is codified in Article 16 TFEU and Article 39 TEU.[53] Besides, Article 8(2) EU Charter stipulates the requirements for an interference with Article 8(1) EU Charter in a broad way. Paragraph 2 particularly requires data controllers and data processors to process the personal data "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Hereby, the EU Charter provides the legislator with a certain margin of appreciation for determining the legitimate aim in correspondence with Article 52 (1) EU Charter that may justify an interference with the fundamental right to data protection for reasons of general interest.[54] Article 52 (1) EU Charter requires that any limitation must be provided for by law and respect the essence of the fundamental rights and freedoms. The European Convention on Human Rights, on the contrary, provides a more specific list of legitimate aims in Article 8 (2) ECHR.

3.3.2.2.2.1 Right to consent, Article 8(2) EU Charter

The concept of informed consent has a pivotal role in medicine and within the data protection framework.[55] In particular Article 8 (2) EU Charter underlines the importance of consent for the protection of the citizens' fundamental rights. This paragraph stipulates that personal data must be processed fairly "on the basis of the consent of the personal concerned or some other legitimate basis laid down by law", while Article 3 (2) EU Charter safeguards the patients' consent to medical treatment. Article 3 EU Charter guarantees the right to respect an individual's physical and mental integrity in general, whereby, in particular in the fields of medicine and biology, free and informed consent must be respected as per Article 3 (2) EU Charter. Citizens have to consent to two distinct conditions, once to the medical examination

v. Sweden, Reports of Judgments and Decisions 1997-IV, 27.08.1997, para. 38, 42, and 43.

[52] Gonzalez Fuster G (2015) "Curtailing a right in flux: restrictions of the right to personal data protection" in: Artemi Rallo Lombarte and Rosario Gracia Mahamut (eds.), "Hacia un nuevo régimen europeo de protección de datos. Towards a new European Data Protection Regime" Tirant lo Blanch (2015), p. 515.

[53] Kranenborg H (2014) Art 8 – Protection of Personal Data. In: S. Peers, T. Hervey, J. Kenner & A. Ward (Eds.). The EU Charter of Fundamental Rights: A Commentary (pp. 223–266). London: Hart Publishing, para. 08.08.

[54] Kokott J, Sobotta C(2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law. Vol. 3. No. 4, p. 224.

[55] Mantovani E, Quinn P (2014) mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology. Vol. 28, No. 2, 222–236, p. 222. http://dx.doi.org/10.1080/13600869.2013.801581.

affecting their physical or mental integrity as well as to the processing of their patient data.

3.3.2.2.2.2 Right to access to personal data, Article 8(2) EU Charter

The right of access to personal data is explicitly enshrined in Article 8(2) EU Charter and falls within the scope of the right to private and family life according to Article 8 ECHR[56]. The CJEU repeatedly confirmed that legislation not offering any opportunity for individuals to seek legal remedies in order to get access to their personal data, or to have their data rectified or erased, does not respect the essence of the fundamental right to effective judicial protection as laid down in Article 47 EU Charter.[57] Article 47(1) EU Charter in particular safeguards the right to an effective remedy for everyone whose rights and freedoms guaranteed by EU law have been violated. The existence of effective judicial review, pursuing to guarantee compliance with EU legislation, has been considered to be intrinsic to the rule of law.[58] To this end, national Data Protection Authorities play an imperative role for respecting citizen's rights, as they, for instance, own the competence to authorize access to specific national data spaces (e.g. French Health Data Hub).[59]

3.3.2.2.2.3 Towards a fundamental right to data security?

The implementation of data security measures serves the protection of multiple fundamental rights. By securing sensitive personal data from unintended disclosure, the confidentiality of personal data in respect of the right to medical confidentiality and the right to protection of one's personal data can be maintained. Although Article 8 EU Charter does not explicitly protect the right to data protection through the implementation of data security measures, the CJEU considers technical and organizational measures to be an essential part of the right to data protection. In the case of *Digital Rights Ireland*, the CJEU argued that the essence of the fundamental right to data protection was not interfered with as the Data Retention Directive foresaw the implementation of data protection principles and data security measures. The CJEU approach towards a data security oriented protection of the fundamental right to data protection has been subject to criticism. For instance, *Brkan*[60] emphasized that the need for the implementation of data security measures, i.e. technical and organizational measures, are not codified in Article 8 EU Charter, and that subsequently data security measures cannot form part of the essence of this fundamental right. Despite this criticism, it is worth observing that also the jurisprudence of the ECtHR acknowledges the importance of safeguards when processing personal sensitive data. In the case of *M.M v. the United Kingdom,* the ECtHR recognized the increasing importance of the safeguards' content where a great amount of

[56] ECtHR, Case of K.H. and Others v. Slovakia, para. 36.
[57] Judgment of 16 July 2020 of the CJEU, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, para 187; Judgment of 6 October 2015 of the CJEU, Schrems, C-362/14, EU:C:2015:650, para. 95.
[58] Judgment of 6 October 2015 of the CJEU, Schrems, C-362/14, EU:C:2015:650, para. 95
[59] EDPS (2020) Preliminary Opinion 8/2020 on the European Health Data Space, p. 12.
[60] Brkan M (2019) The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal (2019), 20, pp. 864–883. Doi:10.1017/glj.2019.66, p. 878-879.

sensitive data is stored on recording systems.[61]

3.3.2.3 Right to medical confidentiality

The provision of healthcare has traditionally been shaped by the patient-doctor relationship and the resulting protection of the patient's data. Patient data may cover any kind of information about individuals related to their past, current or future health or illness. What distinguishes the scope of protection of health data in general from the scope of protection of health data that is being processed in the medical context, is, that the latter enjoys the additional protection of confidentiality legislation besides privacy and data protection legislation. In other words, the processing of health data outside the medical context is subject to the fundamental right to privacy and the right to protection of personal data, whereas the processing of health data in the medical matters enjoys the right to medical secrecy as well. The doctor-patient relationship is characterized by a special relationship of trust, and doctors, in principle, ought not pass on any kind of information about their patients to other people and the public without the patients' permission. The medical confidentiality, thus, adds another layer of protection for the good of the patients and the handling of their data, comprised of an ethical as well as a legal dimension. The principle of confidentiality could therefore be considered as a right of the patient and an obligation of the doctor.[62]

3.3.2.3.1 Protection of medical confidentiality at the European level

Medical confidentiality finds its ethical basis in the Hippocratic Oath, which commands the duties and principles ascribed to physicians. The Declaration of Geneva, adopted in 1948, builds upon the Hippocratic Oath as a modernized version thereof, safeguarding the ethical obligations of care providers independent of the technological evolution.[63] Furthermore, the duty of physicians to maintain the confidentiality of personal information of research subjects is enshrined in the Declaration of Helsinki.[64]

At the European level, Article 8 ECHR protects the right to secrecy concerning an individual's medical state and the transmission of such data to other third parties (regardless of the intended use).[65] As stated above, the European Court of Human Rights considered the confidentiality of health data as a "vital principle" in its case law, which pursues to maintain

[61] ECtHR, Case of M.M. v UK, Judgement (Application no. 24029/07), 13 November 2012, para. 200.
[62] Irish Medical Organisation (2011) IMO Role of the Doctor Series – Doctor-Patient Confidentiality. p. 2. Available here: https://www.imo.ie/news-media/publications/Doctor-Patient-Confidentiality.pdf
[63] World Medical Association, Declaration of Geneva. https://www.wma.net/what-we-do/medical-ethics/declaration-of-geneva/
[64] World Medical Assosication (2018) Ethical Principles for Medical Research Involving Human Subjects. Available here: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/
[65] European Anti-Fraud Office (OLAF), Data Protection Officer (DPO) (2016) Summaries of EU Court Decisions Relating to Data Protection 2000-2015. p. 35. <https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf>

the trust in the medical profession and in healthcare services more generally.[66] Considering the enormous impact that the breach of confidentiality can have on a person's social and professional life, the court requires to take into account the weight of such consequences for an individual when balancing the interests. For instance, in the case of *Y. v. Turkey,* the European Court of Human Rights emphasised that if information about a serious disease, such as HIV, is being revealed, the "interests in protecting the confidentiality of such information will […] weigh heavily in the balance in determining whether the interference is proportionate to the legitimate aim pursued".[67] In light of the ECtHR case-law, such interference may only be "justified by an overriding requirement in the public interest".[68]

3.3.2.3.2 Protection of medical confidentiality at national level

Given that the competence to healthcare remains a national matter, the physicians' duty of confidentiality is primarily protected at the national level and generally embedded in the domestic rules of conduct of medical profession[69]. The following section will therefore explore the protection of medical confidentiality in Germany, Austria, Ireland, and the United Kingdom.

3.3.2.3.2.1 Germany

In Germany, medical confidentiality entails that physicians have to remain silent about the information that they obtained about their patients, which is embedded in the German Criminal Code and the professional code of conduct of the respective medical association of the region *(Länder).* In particular, section 203 (1) Nr. 1 German Criminal Code regulates in conjunction with section 9 of the professional code of conduct[70] that physicians and members of another healthcare profession, who unlawfully discloses

> "another's secret, in particular a secret relating to that person's personal sphere of life or to a business or trade secret which was revealed or otherwise made known to them in their capacity as a physician […] or member of another healthcare profession which requires state-regulated training to engage in the profession or to use the professional title […]"

fears a penalty of imprisonment for up to one year or a fine.

Physicians are therefore required to not share any information, whether it has been shared in oral or written form, that they have been received in their capacity as a physician. Section 9

[66] ECtHR, Case of Z. v. Finland, Judgement (Application no. 22009/93), 25.02.1997.
[67] ECtHR, Case of Y. v. Turkey, Judgement (Application no. 648/10), 17.02.2015, para. 68. See also ECtHR, Case of Z. v. Finland, Judgement (Application no. 22009/93), 25.02.1997, para. 96; .
[68] Ibid.
[69] For instance, in Germany, the rules of conduct of medical profession is transposed by the federal state (*'Bundesland'*); e.g. Sec 9 Rules of conduct of medical profession of Baden-Wuerttemberg.
[70] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte MBO-Ä 1997 – in der Fassung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt geändert durch Beschluss des Vorstandes der Bundesärztekammer am 14.12.2018. Available here: https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/MBO/MBO-AE.pdf

of the professional code of conduct however also stipulates certain exceptions allowing to reveal the patients' information. This may be the case, for instance, if the physician at stake has been released from the patient-doctor confidentiality or is subject to obligatory disclosure (e.g. according to the infection protection law)[71], or if multiple physicians provided treatment to the patient[72]. The latter only applies to the extent that the patient has agreed to the release from the duty of confidentiality or if the consent of the patient can be assumed.

Interestingly, until recently, the German conduct on medical profession prohibited physicians to conduct medical treatments through telehealth, thereby aiming at preventing treatments based on the patients' description, and hence solely their subjective perception. On the federal level, this prohibition has been lifted, whilst the final decision weather remote treatment remains should be allowed remains at the respective medical association of the region (*Länder*).[73] While most regions decided to permit remote treatments partially or fully, the state Brandenburg opposed to allow solely remote treatment. Consequently, this has led to a distribution concerning the admission of remote treatments.[74]

3.3.2.3.2.2 Austria

Section 54 (1) of the Federal Physicians Act[75] bounds physicians and their assistants to secrecy in terms of all secrets that have been entrusted to them or that became known to them in the exercise of their profession. Also, section 121 of the Austrian Criminal Code regulates that secrets related to the health of a person that have been entrusted or made accessible by virtue of their profession in the exercise of a health profession shall be punished by imprisonment up to 6 months or by a fine if the secret has been disclosed or exploited.[76]

Exceptions to the duty of confidentiality are regulated in section 54 (2-6) of the Federal Physicians Act. For instance, such exceptions may apply if physicians are obliged by law to report on the patients' health (Nr. 1) or if the patient has released the physician from their duty of confidentiality (Nr. 3). It is worth mentioning that section 54 (2) (Nr. 4) allows the disclosure of confidential information about the patient if it is necessary for the protection of higher interests of public healthcare or the administration of justice.

3.3.2.3.2.3 Ireland

The confidentiality of care providers is often based on a contractual confidentiality clause, while healthcare practitioners are also bound to common-law duty and have to abide to

[71] Section 9 (2) (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte MBO-Ä.
[72] Section 9 (5) (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte MBO-Ä.
[73] Katzenmeier C (2019) Haftungsrechtliche Grenzen ärztlicher Fernbehandlung, NJW 2019, 1769.
[74] Katzenmeier C (2019) Haftungsrechtliche Grenzen ärztlicher Fernbehandlung, NJW 2019, 1769.
[75] Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte (Ärztegesetz 1998 – ÄrzteG 1998), StF: BGBl. I Nr. 169/1998. Available here: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10011138
[76] Section 121 Strafgesetzbuch, BGBl. Nr. 60/1974 zuletzt geändert durch BGBl. I Nr. 152/2004. Available here: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40059912

Medical Council guidance, demanding to the patients' confidentiality.[77]

The Irish Medical Council's "Guide to Professional Conduct and Ethics for Doctors" provides guidelines with regard to the sharing of patient data, which requires, inter alia, that the disclosure of personal data must be necessary and the recipient must be subject to confidentiality obligations him- or herself.[78] These guidelines also guide on the execution of telemedicine.[79] Notably, the Medical Council's guide requires the collection and processing of data concerning health as the absence of such would result in a breach of the guide at stake.[80]

3.3.2.3.2.4 The United Kingdom

The legislations protecting the medical confidentiality of patient data in the UK is covered by the Common Law Duty of Confidentiality.[81] The guidelines on confidentiality by the General Medical Council explicitly refer to the data protection requirements laid down in the UK Data Protection Act as a complementary means that goes hand in hand with medical confidentiality. However, the common law is an evolutive instrument that progresses with the integration of binding precedents established through case law. It sets out the general rule that obliges doctors to remain silent about the patient information collected. While doctors are generally required not to reveal confidential information about the patient, the common law recognises in principle the patients' consent, statutory obligations, or the public interest as exceptions to the norm.[82] Additionally, confidential patient information may be processed for a specific purpose, such as scientific research or other vital activities, without obtaining the consent of the patient. To this end, the independent Confidentiality Advisory Group (CAG) can permit the use of confidential patient data according to section 251 of the NHS Act 2006 when it becomes unfeasible to obtain consent from the patient.[83] However, the legislation regulating the disclosure or making available of confidential information seems to differ between the four countries within the United Kingdom which adds another layer of

[77] Medical Protection Society (2012) Medical records in Ireland – An MPS Guide, p. 12. https://www.medicalprotection.org/docs/default-source/pdfs/booklet-pdfs/ireland-booklets/medical-records-in-ireland---an-mps-guide.pdf?sfvrsn=29324eac_2

[78] Medical Council (2019) Guide to Professional Conduct and Ethicsfor Registered Medical Practitioners (Amended), p. 24-25. https://www.medicalcouncil.ie/news-and-publications/reports/guide-to-professional-conduct-and-ethics-for-registered-medical-practitioners-amended-.pdf

[79] Ibid., p. 32.

[80] Irish College of General Practitioners (2019) Processing of Patient Personal Data: A Guidelines for General Practitioners v2.3, p. 8. https://www.icgp.ie/speck/properties/asset/asset.cfm?type=Document&id=07BFBD54-DBE7-4EF3-8A60D884D2AA4EE7&property=document&filename=GP_GDPR_Guideline_v2_3..pdf&revision=tip&mimetype=application%2Fpdf&app=icgp&disposition=inline

[81] NHS Digital, protecting patient data. https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data

[82] Ibid., p. 57.

[83] NHS Digital, protecting patient data. https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data

complexity.[84]

3.3.2.3.2.5 Interim conclusion

Each national legislation shows that the principle of confidentiality is not absolute. Disclosure of secret information may be compulsory by law or needs to be weight against various considerations, including the protection of the public interest or the well-being of the patient. However, it becomes obvious that a tension between the sharing of data and the physician-patient confidentiality exists.

3.3.2.4 Right to healthcare

Article 35 EU Charter guarantees the right to health care and obliges the EU to provide a "high level of protection of human health". The right is connected with many other human rights enshrined in the charter, such as the right to human dignity (Article 1 EU Charter), the right to respect for private and family life (Article 7 EU Charter) and the right to protection of personal data (Article 8 EU Charter).[85] To assure the highest level possible for human health and healthcare under Article 35 EU Charter, a European Charter of Patients' Rights[86] was created by non-profit organisations from twelve EU Member States in 2002. The charter determines fourteen patients' rights, namely:

- Right to preventive measures;
- Right of access to health services;
- Right to information regarding the patients' state of health;
- Right to consent;
- Right to free choice among different treatment procedures and providers;
- Right to privacy and confidentiality of personal information, including one's health;
- Right to respect of patients' time;
- Right to the observance of quality standards;
- Right to safety;
- Right to innovation;
- Right to avoid unnecessary suffering and pain;
- Right to personalized treatment;
- Right to complain;
- Right to compensation whenever one suffered harm cause by a health service.

[84] General Medical Council (2017) Confidentiality: good practice in handling patient information, para. 5. Available here: https://www.gmc-uk.org/-/media/documents/gmc-guidance-for-doctors---confidentiality-good-practice-in-handling-patient-information----70080105.pdf?la=en&hash=08E96AC70CEE25912CE2EA98E5AA3303EADB5D88

[85] Hervey, T., & McHale, J. (2014). The Right to Health Care. In S. Peers, T. Hervey, J. Kenner & A. Ward (Eds.). The EU Charter of Fundamental Rights: A Commentary (pp. 951–968). London: Hart Publishing. Para 35.03, p. 952.

[86] European Charter of Patients' Rights, Basis Document, Rome, November 2002, p. 1. https://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf

While the creation of a European Charter of Patients' Rights is generally admirable, it seems to explain the enjoyment of these rights only on a high-level. Furthermore, it does not refer to potential ethical or legal implications that are accompanied with the use of eHealth technologies. However, it is essential to acknowledge that healthcare is a matter of national competence and, subsequently, that the European Union does not have the competence to govern patients' rights. This complicates the achievement of a common Patients' Charter at EU level.

3.3.3 Confidentiality, privacy, data protection legislations and policy instruments at International, European, and EU level

The medical secrecy ruled by the ethical value of the Hippocratic Oath has, initially, been considered as the only necessary protection of the patients' privacy and their medical information.[87] Even though the EU does not have a competence on healthcare matters, the European Union legislator has a certain influence in terms of the protection of the patients' health data as the processing of health data falls is subject to data protection legislation. At the EU and European level respectively, the GDPR and the CoE recommendation on the protection concerning the processing of health-related data (as soft-law) introduce data subject's rights, both frameworks provide derogations and a margin of appreciation to the Member States in restricting the data subject's rights, for instance, for processing activities conducted in the public interest or for the benefit of scientific research[88]. The following sections will therefore explore legislative and non-legislative instruments pertinent to eHealth technologies and the protection of patients' rights.

3.3.3.1 At EU level: Legislations pertinent to the protection of healthcare rights in the eHealth sector at EU level

At the EU level, the GDPR plays a pivotal role concerning the transfer of health data which ought to be applied to a wide range of new technologies, including eHealth services. The regulation came into force in 2018 replacing the Data Protection Directive[89], aiming at protecting the right to data protection while ensuring the free flow of personal data within the European Union. In particular, the GDPR establishes responsibilities to be followed by data controllers and data processors (e.g. data protection principles), and provides citizens

[87] Hohmann J., Benzschawel S. (2013) Data Protection in eHealth Platforms. In: Beran R. (eds) Legal and Forensic Medicine. Springer, Berlin, Heidelberg, p. 1641.

[88] For example, article 89(2) GDPR allows Member States to derogate from the rights referred to in articles 15, 16, 18 and 21 GDPR and the safeguards according to article 89(1) GDPR in terms of data processing for scientific or historical research purposes or statistical purposes if these rights "rights are likely to render impossible or seriously impair the achievement" of the purposes and if the derogation is necessary to fulfil those purposes. Article 89(3) GDPR enables Member States to derogate under the same conditions from the provisions in articles 15, 16, 18, 19, 20, 21 and article 89(1) GDPR for archiving purposes in the public interest.

[89] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

with data subject rights[90]. Other mechanisms under the GDPR provide further protection such as the duty to notification of a data breach to the supervisory authority or communication of a data breach to the data subject when a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject (Article 33, 34), and/or the conduct of a data protection impact assessment[91] (Article 35).

3.3.3.1.1 General Data Protection Regulation

3.3.3.1.1.1 The concept of personal data

The material scope of the GDPR encompasses the protection of *personal data* which is defined in article 4(1) GDPR as "any information relating to an identified or identifiable natural person ('data subject')". The WP29 has determined four elements to be essential for the concept of personal data, namely any information (1), relating to (2), an identified or identifiable (3), natural person (4). However, the scope of protection granted under the GDPR has been debated among scholar, as it is not always straightforward to determine what kind of data may constitute personal data.[92] Despite the attempt to provide parameters for the interpretation of personal data, the legal uncertainty created through a wide interpretation of the term "personal data", as applied by the EDPB under the GDPR, has said to impede the sharing of health data for scientific research and other purposes.[93]

The problem seems to lie in the complexity linked to the scope of application of the GDPR, namely the delineation between personal data and anonymized data. Neither a legal definition for the term "anonymous data", nor anonymisation techniques are specified by the existing data protection framework. The former WP29 provided guidelines on the techniques for anonymising personal data, which defines anonymised data as anonymous data that was related to an identifiable individual, but where that identification is no longer possible by means reasonably to be used.[94] The underlying rationale of the WP29 (or now the EDPB), i.e. that the results of the anonymization process[95] should be the irreversible deidentification

[90] The data subjects rights are the right to be informed and right of access, right to rectification and erasures, right to restriction of processing, notification obligation, right to data portability, right to object and the right not to be subject to a decision based solely on automated processing, including profiling (art 12-22 GDPR). From the patients' perspective on their subject rights, the directive 2011/24/EU on the patient's rights protects individuals in cross-border healthcare becomes relevant as well.

[91] According to recital 91 GDPR, the processing of personal data concerning patients and clients by an individual physician or healthcare professional shall not be considered as processing on a large scale for which the execution of a DPIA should not be mandatory.

[92] Purtova N (2018) The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Law, Innovation and Technology 10:1.

[93] Groos D, van Veen EB (2020) Anonymised Data and the Rule of Law, EDPL 4/2020, p. 499.

[94] Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques. Adopted on 10 April 2014. 0829/14/EN. WP216, p. 8.

[95] According to the WP29, three criteria specify the robustness of anonymization techniques in order to prevent reidentification permanently through means likely reasonably to be used: (1) the possibility to single out individuals, (2) the possibility to link records relating to an individual, and (3) the possibility to infer information concerning an individual. See: Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, 0829/14/EN, WP216.

of one's personal data, has been considered to be unfeasible.[96] In the case of *Breyer,* the ECtHR highlighted the significance of assessing the definition of personal data. The court applied a wide interpretation of the term personal data according to which dynamic IP addresses could constitute personal data even if an additional information from a third party would be necessary to acquire.[97] The question concerning the delineation of the scope is also of significance for the processing of personal data in the field of research, as some countries (e.g. Germany) oblige researchers to anonymize patient if this is in accordance with the research purpose.[98]

The anonymization of patient data may appear to be an attractive means to protect the confidentiality of health data, and the questions if or when personal data can be considered as anonymized is an important one. The sharing of health data logically leads to an accumulation of (non-)personal data which, if viewed separately, might not be related to one another. Evolving technological advancements facilitate new possibilities to single out, link or interfere personal data about a person. This leads subsequently to the challenge that also non-personal data can be linked and potentially reveal a person's identity. The ongoing collection of data facilitates data to be diverse. However, the diversity of collected data and the capability to set data into connection to one another seems to blur the line between health and non-health data.[99] It follows that non-health data, anonymised data, as well as aggregated data have the potential to expose health information about individuals through big data analytics techniques. This leads to obvious tensions within the data protection framework, impairing fundamental data protection principles such as transparency and accountability. Anonymisation and Pseudonymisation are on-going processes and need to be closely observed in order to ensure consistency and compliance with the law.[100]

3.3.3.1.1.2 The concept of data concerning health

Data concerning health constitutes a subcategory of personal data and requires greater protection due to its sensitivity and potential for misuse. According to Article 4(15) GDPR, data concerning health is defined as "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 GDPR provides further clarification regarding the

[96] *Groos, van Vee* argue that anonymisation for the further use of personal data for research purposes is de facto impossible in light of the EDPB's wide interpretation of the term personal data. The authors furthermore argue that the EDPB would neglect the reidentification test developed in the case C-582/14 – Patrick Breyer v Germany (Breyer) by the CJEU, which supposedly provides more legal certainty due to its risk-based approach. [See: Groos D, van Veen EB (2020) Anonymised Data and the Rule of Law, EDPL 4/2020]

[97] Case of Breyer v. Germany, Judgment (Application no. 50001/12), 30.01.2020.; see also ECtHR, Case of S. and Marper v. the United Kingdom, Judgment (Applications nos. 30562/04 and 30566/04), 04.12.2008 in which the ECtHR held that body tissues and samples are personal data.

[98] Section 27(3) Federal Data Protection Act.

[99] Vayena E et al (2018) Policy implications of big data in the health sector. Bull World Health Organ 2018; 96:66–68. P. 67-68. Doi: http://dx.doi.org/10.2471/BLT.17.197426.

[100] Dove ES(2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics, 46 (2018): 1013-1030, p. 1020.

term “data concerning health”, stating that it should include all data related to the health statues of the individual “which reveal information relating to the past, current or future physical or mental health status of the data subject”. The notion of health data thus follows a broad concept covering data that could unveil an individual’s health status. Notably, the WP29 considers data generated in a professional and medical context as “medical data”, which forms part of the concept of data concerning health.

However, it appears that data concerning health cannot always be easily distinguished from personal data in general. The delineation between both categories has been subject to the academic discussion. For some scholars, the definition of “data concerning health” is so broad that it would “cover almost all personal data, as soon as that data is used to gain information on someone’s health”[101]. This problem has manifest itself through the currently existing Covid-19 crisis, which has highlighted the need for data concerning health but also the challenges that come with the collection of personal data. It has shown that location data, which for itself may not reveal information about an individuals’ health, can be a substantial indicator for a person’s health status. In order to guarantee appropriate protection of the citizens’ health data, national data protection authorities have called for a differentiated assessment between data concerning health and personal data. Despite the criticism, it is worthwhile to mention that such an approach would take into account the risks that eHealth technologies bring with it with regard to the processing of health data. At the same time, however, personal data can reveal information about one’s health regardless of the purpose for which it has been processed. Thus, even when personal data is being processed outside of the healthcare context, information about one’s health may be revealed. For instance, if a person regularly goes to a certain address, this in itself can give clues about an individual’s state of health, for example, if this address belongs to an oncologist. *Dove*, for instance, prefers an approach according to which the GDPR would govern the processing of data depending on its function, meaning on the aspects if the processing activity which has the potential to identify an individual, than on the definition of personal data.[102]

Given the increasing possibility for the collection of personal data in general and non-personal data and the opportunity to link data, the delineation between the different categories of non-personal data, personal data, and data concerning health is being challenged.

3.3.3.1.1.3 Legal basis for the processing of health data in the eHealth context

Every processing activity, including the sharing of personal data, requires a legal basis to be lawful. The GDPR is applicable to data transfers conducted through automatic (e.g. interconnected devices) or non-automatic means in healthcare, research and public health. An exception from the prohibition concerning the processing of special categories of data, stipulated in article 9(1) GDPR, applies where explicit consent for the processing of data concerning health has been given, or where it is necessary to process health data to protect

[101] Mulder T (2019) The Protection of Data Concerning Health in Europe. 5 European Data Protection Law Review 209.

[102] Dove ES (2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics, 46 (2018): 1013-1030, p. 1016.

an individual's vital interest, for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health, treatment or the management of health, for reasons of public interest in the area of public health, or for the purpose of scientific research[103]. Considering that the processing of personal data has to comply with the requirements set out in Article 6 GDPR and the processing of special categories of data with Article 9 GDPR, some have argued that a legal basis as per Article 6 and a legal basis as per Article 9 GDPR have to be cumulatively fulfilled.[104]

3.3.3.1.1.3.1 Consent

Explicit consent is a legal ground for the processing of data concerning health for research purposes that organisations often refer to. Explicit consent has to be free, specific, informed and unambiguous.[105] Recital 33 highlights that it may not always be feasible to identify the research purpose when collecting the personal data and thereby offers a certain degree of flexibility to describe the research purpose more generally with regard to the specification of consent. Nonetheless, it is not always clear how flexibly it can be applied. The EDPB states, for instance, that such flexibility may not strictly be applicable to the processing of sensitive personal data in light of the strict requirements laid down in Article 9 GDPR.[106] It is worth mentioning that the prerequisites of informed consent concerning the participation in scientific research and of explicit consent concerning the processing of personal data in the context of scientific research are two distinct requirements.[107] The notion of consent does not merely have legal significance as it also encompasses an ethical component, representing an act of enforcement of one's personal will and freedom.[108] It is therefore important to consider that the informed consent legitimizing the participation in health research as an "ethical" condition needs to be fulfilled even if another legal basis for the processing of medical data applies.[109]

3.3.3.1.1.3.2 Healthcare

In the healthcare context, data concerning health can be processed where it is "necessary for the purposes of preventive or occupational medicine, for the assessment of the working

[103] Articles 9(a), (c), (h), (i), (j) GDPR.
[104] Dove ES (2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics, 46 (2018): 1013-1030, p. 1016, p. 1020.
[105] Article 9 (2) (a), Article 7 GDPR.
[106] EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, para. 157.
[107] EDPB (2021) EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Adopted on 2 February 2021, para 5.
[108] Mantovani E, Quinn P(2014) mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology. Vol. 28, No. 2, 222–236, p. 223. http://dx.doi.org/10.1080/13600869.2013.801581.
[109] EDPB (2021) EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Adopted on 2 February 2021, para 7.

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". [110] Care professionals who are subject to the obligation of professional secrecy are allowed to process the personal data related to the patient under this provision.[111] They, thus, may collect or share patient data with colleagues without having to rely on the patients' approval in order to provide adequate healthcare services.

3.3.3.1.1.3.3 Scientific research

The health data sharing environment is complex due to the multitude of stakeholders involved, ranging from academic stakeholders to private commercial stakeholders. The notion of scientific research has to be interpreted in a broad manner according to recital 159, which includes, amongst others, technological development, privately funded research, and, more importantly, studies in the public interest in the area of public health. Although the GDPR provides various legal grounds for the processing of data concerning health, scientific research has been privileged because of the existing compatibility clause. Article 6(4) in conjunction with recital 50 GDPR allows the further processing of personal data and special categories, if the purpose for the secondary processing is compatible with the purpose for which the data were initially collected. If special categories of data, such as data concerning health, have been initially processed, then this can indicate the compatibility with the further processing including such data. The GDPR therefore aims to ease the requirements concerning the further processing of data.

3.3.3.1.1.3.4 Public health

Article 168 TFEU sets the fundament for facilitating cooperation in terms of public health between EU Member States.[112] For the EDPS, "eHealth is a key area of public interest where the Commission's Data Strategy envisages the creation of a common space, namely the European Health Data Space ('EHDS')".[113] Even though recital 159 considers public health as a subcategory of scientific research, the GDPR provides an explicit provision to the processing in the interest of public health in Article 9(2)(i) GDPR. The legal basis enumerates examples as regards to what the notion of public health entails (e.g., ensuring standards of quality and safety of healthcare). Recital 54 refers to Regulation (EC) No. 13338/2008, which defines public health as "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."

3.3.3.1.1.4 The data subject's rights

The GDPR provides individuals, including patients, with data subject's rights[114], namely:

[110] Article 9(2)(h) GDPR.
[111] Article 9(2)(h) in conjunction with Article 9(3) GDPR.
[112] EDPS (2020) Preliminary Opinion 8/2020 on the European Health Data Space, p. 8.
[113] EDPS (2020) Preliminary Opinion 8/2020 on the European Health Data Space, p. 6.
[114] Articles 12-22 GDPR.

- The right to information;
- The right to access;
- The right to rectification;
- The right to erasure ("the right to be forgotten");
- The right to data portability;
- The right to object;
- The right to withdraw consent;
- The right not to be subject to automated individual decision-making, including profiling.

These rights are not absolute as the regulation foresees certain restrictions with regard to the data subjects rights. For instance, when controllers and processors exceptionally process (or transfer[115]) data for the provision of healthcare (Article 9(2)(h)), for research (Article 9(2)(j), 89(1)), or reasons of public interest[116] in the area of public health (Article 9(2)(i)), the right to information[117] can be restricted to the detriment of the patient. Article 89 GDPR allows to restrict the data subject's rights, if additional safeguards have been implemented. For instance, the right to erasure can be denied, if it would seriously impede the achievement of the objectives of the research or even make it impossible.[118] Also, the GDPR exempts from the right to object for reasons of public interest laid down in law.[119] Furthermore, Member States are permitted to implement derogations from the data subject rights listed in Article 89(3) GDPR, where they "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".[120]

3.3.3.1.1.5 Data protection principles

The GDPR provides seven principles related to the processing of personal data in Article 5 GDPR.[121] In particular, the principle of confidentiality and integrity can serve patients to maintain the secrecy of their personal data. To this end, cybersecurity requirements aim at maintaining the confidentiality of data through safeguards (i.e. technical and organizational

[115] The GDPR appears to refer to data transfers as 'disclosure by transmission, dissemination or otherwise making available' of data (art 4(2) GDPR). Also, the term 'recipient' (art 4(9) GDPR) seems to refer to data transfers.

[116] Public interest according to recital 45 may cover 'health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.' Recital 54 specifies that public health should be interpreted as defined in Regulation (EC) No 1338/2008. Moreover, the term public interest is defined by jurisprudence of the Court of Justice of the European Union.

[117] See for instance: art 14(5)(b) GDPR.

[118] Article 17(3)(d) GDPR.

[119] Article 21(6), recital 45 GDPR.

[120] Article 89(2) GDPR.

[121] The data protection principles are lawfulness, fairness and transparency(1), purpose limitation(2), data minimization(3), accuracy(4), storage limitation(5), integrity and confidentiality(6), and accountability(7); see Article 5(1-2) GDPR.

measures)[122], thereby constituting a pre-requisite for health data transfers. However, the term confidentiality may have a different meaning under the GDPR than under the national legislations regulating the physicians' duty to confidentiality. The GDPR refers to this term as a technical safeguard with the aim to keep the data secure, for instance, through access controls. According to Article 25 GDPR, appropriate technical and organisation measures should be implemented by default. Besides, recital 78 specifies that the protection of the rights and freedoms of natural persons require the implementation of appropriate technical and organisational measures. With the aim to safeguard rights and freedoms of individuals, one might wonder how the principles of confidentiality under the GDPR relates to the physicians' duty of confidentiality. Furthermore, in the context of data sharing where enormous amounts of data can be exchanged, the principle of data minimisation can support the protection of patients. However, at the same time, this principle stands in contraction to the sharing of data and has the ability to constrain the sharing of patient data in eHealth for the benefit of healthcare, research, and public health.

3.3.3.1.2 Directive on the application of patients' rights in cross-border healthcare

In addition to the GDPR, the Directive on the application of patients' rights in cross-border healthcare[123] becomes relevant for patients who have received *cross-border healthcare within the EU*, for instance, through telehealth applications. In this context, Member States shall be supported in establishing European reference networks and to facilitate the exchange of information and expertise, and in cooperating in the development of diagnosis and treatment of rare diseases[124] as well as in supporting the exchange of information within a voluntary eHealth network connecting national institutions[125]. Especially with regard to the latter, the creation of guidelines containing a non-exhaustive list of data that could be included in patients' summaries and shared among care professionals, as well as establishing methods facilitating the usage of medical data for public health and research could influence and guide the transfer of cross-border sharing.[126] Furthermore, patients who receive cross border healthcare, meaning patients who receive medical treatment in another Member State than in the country of residence, shall have access to their medical record. The directive on patient rights in cross-border healthcare[127] reserves patients the right to a written or electronic medical record concerning the treatment they have received in the other Member State, as well as access to a copy of the medical record.

[122] Here, the Medical Device Regulation 2017/745/EU (replacing the Medical Device Directive 93/42/EEC on 26 May 2021) and the NIS Directive 2016/1148/EU may complement the cybersecurity requirements.
[123] 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.
[124] Article 12(f) Directive on the application of patients' rights in cross-border healthcare.
[125] Article 14 Directive on the application of patients' rights in cross-border healthcare.
[126] Article 14(2)(b)(i and ii) Directive on the application of patients' rights in cross-border healthcare.
[127] 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, OJ L 88, 4.4.2011, p. 45–65.

3.3.3.2 At international level: Draft recommendation on the protection and use of health-related data by the UN Special Rapporteur

On an international level, the *UN Privacy rapporteur* published a draft recommendation on the protection and use of health-related data due to the vast risks associated with the processing of health-related data.[128] The draft recommendation is not legally binding but represents the political will to endorse the protection and use of health-related data. This documents highlights the need for a common international approach in order to achieve a minimum data protection standards for health-related data. The recommendation provides rules concerning the sharing of health-related data for purposes of providing and administering health care and purposes other than the mentioned ones.[129] Besides drafting legal conditions for data processing of health-related data, it also contains specific provisions, amongst others, for scientific research, mobile applications, trans-border flows of health-related data, electronic health records, health-related data and open data, automated decision making, intersectionality and health-related data.[130]

3.3.3.3 At European level

3.3.3.3.1 The Oviedo Convention

The Convention on Human Rights and Biomedicine ("Oviedo Convention")[131] is legally binding at a transnational level, and established to protect human rights and freedoms in the area of biomedical research and medicine. With respect to the right to information, the Oviedo Convention regulates that patients have a right to know about any information that is collected about their health but also have the right to respect their wishes not to be informed.[132] The right not to know founds its basis in Article 10.2 Oviedo Convention. The Council of Europe Recommendation on the protection of health-related data also explicitly encompasses the right not to be informed of a diagnosis and prognosis if the absence of knowledge does not pose a risk to the health of others[133]. The right not to know has also partially been imbedded into national legislations. For instance, the German Civil Code states that, in light of the personality rights, that patients have the right not to know about their genomic imprinting including information about a possible vulnerability to particular illnesses. This negative attribution of the fundamental right to self-determination has also been referred to as fundamental right to bioethical referred to as the fundamental right to bioethical self-determination (*bioethische Selbstbestimmung*)[134]. Furthermore, the obligation

[128] UN (2019) 'Call for contributions: Draft Recommendation on the Protection and Use of Health-Related Data. https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/HealthRelatedData.aspx.
[129] See paragraph 8 and 9 UN draft recommendation (ibid).
[130] See chapter V-VIII, XII, XIII, XXII Draft recommendation (ibid).
[131] Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. ETS No. 164, 01.12.1999.
[132] Article 10(2) Oviedo Convention.
[133] Article 11.7 CoE Recommendation.
[134] Koppernock M (1997) Das Grundrecht auf bioethische Selbstbestimmung. Nomos Verlagsgesellschaft Baden-Baden, p. 89-94.

to inform as per section 630e German Civil Code entails that the information must be provided in a language that the patient understands and, if necessary, to involve an interpreter at the patients expense.[135]

3.3.3.3.2 The Council of Europe recommendation on the protection of health-related data

In light of the transposition of the modernized Convention 108+, the Council of Europe has issued a new recommendation on the protection of health-related data with the aim of solidifying the protection of personal data in respect of human rights, in particular the right to privacy and the right to data protection.[136] The *Council of Europe Recommendation on the protection of health-related data*[137] is thus of particular importance at the European level and calls their member states to integrate the guidelines to both private and public sector actors who process health-related data, including national healthcare professionals and other stakeholder. Notably, however, the recommendation considers "the people's desire to have more control over their personal data and the decisions based on the processing of such data"[138]. The recommendation, according to its wording, aims to achieve this need by involving patients "in understanding the manner in which decisions concerning them are being taken"[139]. Also, in prospect of the benefits that the usage of health-related data brings to public health and personalised patient care, emphasis has been put on the implementation of appropriate state-of-the-art security measures in order to protect patients effectively.[140]

The new recommendation replaces the previous Council of Europe recommendation on the protection of medical data[141] and thereby introduces a broader term, namely "health-related data".

According to the new Council of Europe recommendation, "personal data"

---

[135] Deutscher Bundestag (2012) Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten Drucksache 17/104088, p. 25. Available here: http://dipbt.bundestag.de/dip21/btd/17/104/1710488.pdf

[136] Council of Europe (2019) Protection of health-related data: Council of Europe issues new guidelines, press release. https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168093b57d.

[137] Council of Europe (2019) Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States
on the protection of health-related data (Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies).

[138] Council of Europe (2019) Protection of health-related data: Council of Europe issues new guidelines, press release. https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168093b57d.

[139] Ibid.

[140] Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, 27 March 2019.

[141] Council of Europe, Recommendation No. R(97)5 of the Committee of Ministers to member States on the protection of medical data, 13 February 1997. According to article 2 of the recommendation on the protection of medical data, '"medical data" refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data'.

> *"refers to any information relating to an identified or identifiable individual ("data subject")"*,

whereas "health-related data" is being defined as

> *"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*"[142].

At a first glance, it could seem that the term "health-related data" might offer a wider protection than the term "data concerning health" as provided by the GDPR, as the term seems to be more abstract by suggesting that the data only needs to be *related* to one's health and does not strictly require to *concern* an individual's health. The resemblance of both concepts, however, becomes clearer when reading recital 35 GDPR, which clarifies that "data concerning health should include all data pertaining to the health statues of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject". Thus, both acts seem to guard a similar type of health data. Nonetheless, it may not always be evident what kind of data constitutes health data, and the similarity between both definitions suggests that both instruments struggle with the delineation of the scope of health-related data and data concerning health, respectively.

The recommendation sets out various principles and, as soft-law, permits the processing of health-related data, inter alia, for reasons of public health (e.g. to ensure the quality and safety of medical treatment, health products and medical devices), or the public interest (e.g. scientific research) as defined in Article 5a. In comparison to the GDPR, the recommendation provides more concrete guidelines for the "exchange and sharing of health-related data" (Article 2.1) in the public and private sector, and entails specific provisions regarding data transfer by different professionals for providing and administering health care as per article 8. In particular, the exchange and sharing of health-related data between health professionals should be limited to the information that is necessary for the provision of care. Also, the use of electronic medical files or electronic mailboxes should comply with the principles as per Article 8.4. The recommendation does not clarify the terms "exchange" and "data sharing", but rather refers to "the use of electronic medical files and electronic mailboxes" (Article 8.4). Moreover, it introduces rights of the data subject, which can also deviate from the GDPR. In particular, the data subject's rights are transparency of processing (Article 11), access to data, rectification, erasure, objection to the processing and data portability (Article 12).

3.3.3.4 Proposal for a Regulation on European data governance (Data Governance Act)

In November 2020, the European Commission has published a *proposal for a regulation on European data governance*, the so-called "Data Governance Act"[143]. Its objective is to

[142] Article 3 CoE Recommendation.

[143] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), COM(2020) 767 final, 2020/0340 (COD), SWD(2020) 296 final.

increase the availability and usage of personal and non-personal data. Particularly with regard to the latter, the sharing of personal data is ought to be embraced through different types of intermediaries who's task is "to help individuals exercise their rights under the General Data Protection Regulation (GDPR)"[144], and thereby to strengthen trust in data sharing[145]. Another goal of the proposal is to facilitate the use of data based on altruistic considerations, namely "to collect data for the common good". In this respect, measures that enhance data altruism will be implemented. Organisations processing data for data altruistic purposes shall have the possibility to register as a "Data Altruism Organisation recognised in the EU"[146], and "European data altruism consent forms" will be developed for the processing of data for the purpose of scientific research and statistical use of data. In particular,

> *"data altruism" means the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services"*[147]

The definition merely specifies that the processing for altruistic can be conducted if it takes place in the general interest. The DGA offers some further guidance in its chapter IV in order to enable data altruism, however, it does not provide a definition on the term "general interest"[148]. Further confusion is caused as the DGA introduces in its introductory explanation to be the voluntary making available of data for the common good through individuals or companies[149]. The European Commission thereby uses multiple terms, namely data altruism, general interest, common good, without providing further explanation.

The DGA suggests consent to be typically the appropriate legal basis for the processing of data for scientific research based on data altruism.[150] This is stated to be possible if ethical standards relevant to scientific research are taken into account. It highlights moreover the possibility to further process data for scientific research in light of Article 5 (1) (b) and Article 89 (1) GDPR, specifying the assumed compatibility with the initial purpose. The development of a common European data altruism consent shall in addition ease the portability of data if it is not stored directly by the citizen[151] and foster transparency for individuals with the aim to inform them about how their data is being used and how it could

[144] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance(Data Governance Act), p. 1.
[145] 'Data sharing' means the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary; article 2(7) of the proposal.
[146] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), p. 6.
[147] Article 2(10) of the proposal.
[148] Article 19 (2) DGA only specifies that an entity shall "ensure that the data is not be used for other purposes that those of general interest for which it permits the processing".
[149] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), p. 8.
[150] Recital 38 DGA suggests to rely on Article 6 (1) (a) and 9 (2) (a) in conjunction Article 7 GDPR.
[151] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), p. 8.

be accessed[152]. The EU data altruism consent from is supposed to be adapted to each sector[153].

Despite the currently existing scope for interpretation, enabling the sharing of data for altruistic purposes, offers, in principle, many opportunities to serve the flow of data for the improvement of healthcare, research, and public health. The first reactions towards the DGA, however, are diverse. Some stakeholder encourage the sharing of personal data but criticize that the possibility to share data remains limited in respect of the requirements as currently laid down in the GDPR, which subsequently require modification for the benefit of altruistic data sharing.[154] Others criticize that the DGA includes personal data into its scope of application. This is because the proposal for the DGA has been said to stand in contradiction to the rationale of the GDPR and e-Privacy Directive, shifting the focus from citizen empowerment and to strengthening the data economy.[155]

[152] Recital 39 DGA.
[153] Recital 39 DGA.
[154] Veil W(2020) Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt. CR-online.de Blog.CRonline Portal zum IT-Recht. 01.12.2020. Available here: https://www.cr-online.de/blog/2020/12/01/datenaltruismus-wie-die-eu-kommission-eine-gute-idee-versemmelt/
[155] Feedback from Access Now Europe, Feedback reference F1484899, 29 January 2021, Initiative: Data sharing in the EU – common European data spaces (new rules). Available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules/F1484899

4 Conclusion

There is no complete overlap in terms of ethical principles between biomedical ethics and the underlying ethics of existing confidentiality, privacy, and data protection legislations. The following section will therefore provide an overview of the identified discrepancies between the two. It will also provide an overview on moral dilemmas that result from the above-mentioned discrepancies. These overviews are followed by an examination of legal conflicts within the existing laws.

4.1 Impediment between biomedical ethics and law

The biomedical ethical principle of respect for persons and their autonomy consists of two aspects: the first one is that citizens should have the freedom to make autonomous decisions, such as consenting to share personal data, and the second one is, where their autonomy is diminished, protection of the persons autonomy should be safeguarded, for example when citizens have a medical condition and rely on medical care. In particular the first structure of thought has manifested itself as part of existing confidentiality, privacy, and data protection legislations. It has been said that consent plays a dominant role with regard to the processing of personal data.[156] Informed consent is often perceived as an instrument to exercise control and to manifest a person's free will in respect of their personal autonomy.[157]

When analyzing the existing legislations on data protection closer, it becomes evident that the citizens' right to access and the right to data portability are rights which facilitate citizens to actively access their data and to share it with other stakeholders. However, this does not hold true in the same extent when it comes to the right to data portability. There it is only applicable where the processing has been based on consent or on a contract. This restricts the citizens' autonomy in their choices to actively share their personal data where the processing has taken place on the legal ground of scientific research or in the public interest. This means that in certain cases, the first aspect of the ethical principle is eroded in a sense and that this is often the case when there is a disparity between the data subject and the data holder.

There also other situations where the citizens' autonomy is weakened, while the respective legislations only provides partial protection: for instance, data protection legislation allows to restrict the data subject's rights when processing data for scientific research, if additional safeguards (e.g. pseudonymisation or even anonymisation of personal data) have been implemented.[158] These measures have, in principal, the potential to protect a person's autonomy where he or she is not able to autonomously influence the use of the data. Respect for autonomy, however, can also conflict with other moral values that can supersede these

[156] Kranenborg H (2014) Art 8 – Protection of Personal Data. In: S. Peers, T. Hervey, J. Kenner & A. Ward (Eds.). The EU Charter of Fundamental Rights: A Commentary (pp. 223–266). London: Hart Publishing, para.. 08.25.

[157] Biasin E, Brešić D, Kamenjašević E, Notermans P, SAFECARE. Analysis of ethics, privacy, and confidentiality constraints, Deliverable 3.9, p. 69. Available here: https://www.safecare-project.eu/wp-content/uploads/2020/02/Analysis-of-Ethics-Privacy-and-Confidentiality-Restraints.pdf

[158] See, for instance, Article 89 GDPR.

principles. This is the case when restrictions on the data subject's rights deprive citizens from their ethical duty to share their data. If they are not capable of getting access to it or porting it, then this incapability may lead to a conflict with the principle of benevolence.

Another important ethical principle, the principle of justice, has shown that legislation might need to consider the special needs of the most vulnerable. As of yet, confidentiality, privacy, and data protection legislation lacks provisions that supports, for instance, the sharing and processing of health data on rare diseases. The notion of scientific research is broad and encompasses various research activities conducted by private and public actors. Even though data protection legislation does not abandon the research for rare diseases, researchers may favour to research about wide spread diseases. In particular, private stakeholders presumably have a tendency to choose research projects that have the potential for economic profit, meaning that common diseases might become favoured research objects. Under consideration of the principle of distributive justice, researchers may be ethically obliged to ensure that the most vulnerable citizens are being considered. Furthermore, the principle of distributive justice may also encompass an ethical obligation to ensure access to eHealth technologies to financially disadvantaged or citizens with medical conditions in order to ensure the access to healthcare.

Yet another principle, the principle of beneficence, requires citizens to provide good to other citizens. The proposal on the DGA, in general, provides a favourable step, which serves the achievement of benevolent behaviour and the sharing of citizens' data for the good of others, namely to share data for altruistic purposes. Also, the currently existing data protection legislations enable to process data for scientific research, healthcare, and the public interest which may constitute subcategories of altruistic reasons. Moreover, as mentioned before, the right to access and the right to data portability are enablers that enhance the ethical duty of individuals to share data. Besides this, the principle of beneficence could oblige citizens to use eHealth technologies. For instance, some countries are in the process of deploying electronic health records but have yet not been able to fully implement eHealth technologies. This hinders the possibility to fulfil the duty to use eHealth technologies and subsequently to share health data. Nonetheless, a duty to use and share data may exist only insofar as it is not disproportionate. This might be the case where the sharing of health data may pose a significant risk to the citizens' rights and freedoms. The unintended disclosure of health information could lead to the stigmatisation of individuals based on sensitive information about certain disease within their societal environment and may even lead to the refusal of insurance coverage. Economic and societal harm could result from discrimination and diminish the opportunities in the economic market when applying for jobs or concluding contracts. It is therefore necessary to handle and safeguard the data properly.[159]

[159] Verhenneman G, Vedder A, WITDOM, Legal and Ethical framework and privacy and security principles. Deliverable 6.1, p. 43. Available here: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6%201_Legal%20and%20EthicalFrameworkand%20Privacy%20and%20Security%20Principles_v1.0_final_20150630.pdf

Finally, the principle of non-maleficence is a prominent example of how biomedical ethical values can contradict one another, especially when it comes to the sharing of patient data and the physicians' duty to confidentiality. The analysis has shown that the concept of medical secrecy follows the objective to protect the citizens' conviction in the medical professionals and the healthcare system in general, but it has also shown that the exceptions to the duty of confidentiality exist and, hence, that it is not an absolute right.

Against this backdrop, national legislations have codified various exceptions to the obligation of medical secrecy, most commonly covering reasons such as statutory obligations, the exchange of health information with other care providers in the interest of citizens or the sharing of patient information in the interest of public health. While some countries enable the sharing of patient data for the benefit of public health, the sharing of health data by physicians for the benefit of improving healthcare and medical research does not seem to be allowed under the national confidentiality legislations that were considered above. Furthermore, the principle of non-maleficence may oblige citizens not to pose the risk to harm others and thereby require them to refrain from sharing data related to other people. This duty generally restricts the duty to share data related to their health.

4.2 Conflicts within the law

The legal analysis shows that the legal framework of fundamental rights embedded in various legislations at European, EU and national level provides a profound protection of citizens' rights when it comes to data sharing in eHealth. In particular, individual protection is being guaranteed on a national level through federal laws and fundamental rights, either explicitly embedded in national basic law or implicitly safeguarded through constitutional case law. The protection of patients' rights is guaranteed through various rights, such as the right to self-determination, right to dignity and the right to treatment. This protection is initially of social nature, taking into account the risks that the exposure of sensitive medical information poses to the patients' dignity. The data subject's rights provided by the GDPR specify or expand these rights, taking into account the increasing use of eHealth technologies in medicine.

Furthermore, a conflict within the existing data protection framework occurs when it comes to health data sharing. The legal examination of the most prominent data protection legislation, i.e. the GDPR, has shown that the sharing of health data violates data protection principles (e.g. the principle of data minimisation). Additionally, citizens are currently not able to fully exercise control over their personal health data because of the possible restrictions imposed regarding the data subject's rights under the GDPR.

Finally, a third conflict between the data protection framework and future legislative endeavours has been identified. It manifests itself particularly when exploring the relationship between the GDPR and the DGA. While the European Commission promotes the DGA to enhance data sharing practices for the public good with the aim to support the implementation of sectoral data spaces at EU level, the GDPR aims to protect the processing of personal data of individuals, including citizens. The interests that the DGA pursues do not

seem to be new to the GDPR. While the DGA seems to rely merely on consent as a legal basis to process personal data for altruistic purposes, the GDPR sets out a variety of legal bases beyond consent, thereby aiming at balancing societal interests with the interest of individuals when processing personal data. To enable lawful processing, the GDPR permits amongst other things the processing of personal data for scientific research and public health. Both instruments, the DGA and the GDPR, thus seem to overlap to a certain extent as the processing of personal data for scientific research and the public interest under the GDPR could also be considered to serve altruistic purposes. With that in mind, the question arises if and to what extend the personal data processed under the aforementioned requirements of the GDPR can be used for the processing of altruistic purposes under the DAG. Here, problems may arise as the rationale behind both instruments seem to contradict each other, shifting the focus from the protection of individuals and their digital rights towards the enhancement of data economic interests. Against this backdrop, the DGA requires further clarification on certain terminologies in order to address the existing legal uncertainty resulted from the absence of specific definitions (e.g. data intermediaries, general interest).

References

Article 29 Data Protection Working Party (2017) Guidelines on the right to data portability. Adopted on 13 December2016 As last Revised and adopted on 5 April 2017. WP 242 rev.01.

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, 0829/14/EN, WP216.

Article 29 Working Party (2015) ANNEX 'health data in apps and devices' to the letter of the WP29 to the European Commission on the clarification of the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

Beauchamp TL, Childress JF (1979) Principles of Biomedical Ethics, Oxford University Press.

Biasin E, Brešić D, Kamenjašević E, Notermans P, SAFECARE. Analysis of ethics, privacy, and confidentiality constraints, Deliverable 3.9. Available here: https://www.safecare-project.eu/wp-content/uploads/2020/02/Analysis-of-Ethics-Privacy-and-Confidentiality-Restraints.pdf

Boogerd EA et al (2015) "What Is eHealth": Time for an update?. JMIR Res Protoc 2015;4(1):e29.

Brigida R et al (2017) Ethical sharing of health data in online platforms – which values should be considered?. Life Sci Soc Policy. 2017 Dec; 13:12. Doi: 10.1186/s40504-017-0060-z.

Brkan M (2019) The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. German Law Journal (2019), 20, pp. 864–883. Doi:10.1017/glj.2019.66.

Callens S (2019) The demand for new legislation on eHealth in the EU, in: Bächle TC, Wernick A (eds) The futures of eHealth: Social, Ethical and Legal Challenges, 135-141. Alexander von Humboldt Institute for Internet and Society (HIIG).

Choudhry S (2014) Right to Respect for Private and Family Life (Family Life Aspects). In S. Peers, T. Hervey, J. Kenner & A. Ward (eds.). *The EU Charter of Fundamental Rights: A Commentary* (pp. 183-222) London: Hart Publishing, article 7, para 0718B1.

Council of Europe (2015) Introductory report for updating recommendation R(97) 5 of the council of Europe on the protection of medical data by Jeanne Bossi Malafosse. T-PD(2015)07. 3.

Department of Health & Social Care (2021) The NHS Constitution for England. Available here: https://www.gov.uk/government/publications/the-nhs-constitution-for-england

Deutscher Bundestag (2012) Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten Drucksache 17/104088. Available here: http://dipbt.bundestag.de/dip21/btd/17/104/1710488.pdf

Di Fabio U (2001). In: Maunz, Theodor/ Dürig, Günter (eds) Grundgesetz Kommentar, Verlag C.H. Beck Müchen.

DIGITALEUROPE (2020) Harnessing the power of AI in health applications – How EU policies can foster the development of an ethical and trustworthy AI to bring better health to citizens, 14.01.2020. Available here: https://www.digitaleurope.org/resources/harnessing-the-power-of-ai-in-health-applications/

Dove ES (2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics, 46 (2018): 1013-1030.

EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020.

EDPB (2021) Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Adopted on 2 February 2021.

EDPS (2020) Preliminary Opinion 8/2020 on the European Health Data Space, 17.11.2020. Available here: https://edps.europa.eu/sites/edp/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf 13.

European Anti-Fraud Office (OLAF), Data Protection Officer (DPO) (2016) Summaries of EU Court Decisions Relating to Data Protection 2000-2015. <https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf>

European Charter of Patients' Rights, Basis Document, Rome, November 2002. Available here: https://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf.

European Commission (2018) 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; empowering citizens and building a healthier society COM(2018) 233 final.

European Commission (2018) Ethics and data protection. 14 November 2018. Available here: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf.

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, COM(2018) 233 final, SWD(2018) 126 final.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, SWD(2015) 100 final.

European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), COM(2020) 767 final, 2020/0340 (COD), SWD(2020) 296 final.

European Commission (2016) Patients' Rights in the European Union Mapping eXercise. Final Report. Available here: https://ec.europa.eu/health/sites/health/files/cross_border_care/docs/2018_mapping_patientsrights_frep_en.pdf

European Court of Human Rights (2015) "Health-related issues in the case-law of the European Court of Human Rights", Thematic Report.

European Parliament (2021) Public Health – Fact Sheets on the European Union - 2021. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/49/public-health

Faiella G et al, Building an Ethical Framework for cross-border applications: the KONFIDO project. Available here: https://konfido-project.eu/sites/default/files/publications/5faiellaethicalframework.pdf

Feedback from Access Now Europe, Feedback reference F1484899, 29 January 2021, Initiative: Data sharing in the EU – common European data spaces (new rules). Available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules/F1484899

General Medical Council (2017) Confidentiality: good practice in handling patient information. Available here: https://www.gmc-uk.org/-/media/documents/gmc-guidance-for-doctors---confidentiality-good-practice-in-handling-patient-information---70080105.pdf?la=en&hash=08E96AC70CEE25912CE2EA98E5AA3303EADB5D88

Gonzalez Fuster G (2015) "Curtailing a right in flux: restrictions of the right to personal data protection" in: Artemi Rallo Lombarte and Rosario Gracia Mahamut (eds.), "Hacia un nuevo régimen europeo de protección de datos. Towards a new European Data Protection Regime" Tirant lo Blanch (2015).

Groos D, van Veen EB (2020) Anonymised Data and the Rule of Law, EDPL 4/2020.

Hervey, T., & McHale, J. (2014). The Right to Health Care. In S. Peers, T. Hervey, J. Kenner & A. Ward (Eds.). The EU Charter of Fundamental Rights: A Commentary (pp. 951–968). London: Hart Publishing. Para 35.03.

Hohmann J., Benzschawel S. (2013) Data Protection in eHealth Platforms. In: Beran R. (eds) Legal and Forensic Medicine. Springer, Berlin, Heidelberg.

Irish College of General Practitioners (2019) Processing of Patient Personal Data: A Guidelines for General Practitioners v2.3. https://www.icgp.ie/speck/properties/asset/asset.cfm?type=Document&id=07BFBD54-DBE7-4EF3-8A60D884D2AA4EE7&property=document&filename=GP_GDPR_Guideline_v2_3..pdf&revision=tip&mimetype=application%2Fpdf&app=icgp&disposition=inline

Irish Medical Organisation (2011) IMO Role of the Doctor Series – Doctor-Patient Confidentiality. Available here: https://www.imo.ie/news-media/publications/Doctor-Patient-Confidentiality.pdf

Katzenmeier C (2019) Haftungsrechtliche Grenzen ärztlicher Fernbehandlung, NJW 2019, 1769.

Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law. Vol. 3. No. 4.

Koppernock M (1997) Das Grundrecht auf bioethische Selbstbestimmung. Nomos Verlagsgesellschaft Baden-Baden, p. 89-94.

Kranenborg H (2014) Art 8 – Protection of Personal Data. In: S. Peers, T. Hervey, J. Kenner & A. Ward (Eds.). The EU Charter of Fundamental Rights: A Commentary (pp. 223–266). London: Hart Publishing.

Mantovani E, Quinn P (2014) mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology. Vol. 28, No. 2, 222–236. http://dx.doi.org/10.1080/13600869.2013.801581.

Medical Council (2019) Guide to Professional Conduct and Ethics for Registered Medical Practitioners (Amended). Available here: https://www.medicalcouncil.ie/news-and-publications/reports/guide-to-professional-conduct-and-ethics-for-registered-medical-practitioners-amended-.pdf

Medical Protection Society (2012) Medical records in Ireland – An MPS Guide. https://www.medicalprotection.org/docs/default-source/pdfs/booklet-pdfs/ireland-booklets/medical-records-in-ireland---an-mps-guide.pdf?sfvrsn=29324eac_2

Mulder T (2019) The Protection of Data Concerning Health in Europe. 5 European Data Protection Law Review 209.

NHS Digital, protecting patient data. https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data

Norman CD, Skinner HA (2009) eHealth Literacy: Essential Skills for Consumer Health in a Networked World. Journal of medical Internet research vol. 8,2 e9. Doi:10.2196/jmir.8.2.e9.

Ombudsman (2012) The Ombudsmans Statement of Good Practice for the Public Health Service in Dealing with Patients. Available here: https://www.ombudsman.ie/publications/reports/a-report-by-the-ombudsman/

Purtova N (2018) The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Law, Innovation and Technology 10:1.

Riazul Islam SM et al (2015) The Internet of Things for Health Care: A Comprehensive Survey 3 IEEE Access 678.

UN (2019) 'Call for contributions: Draft Recommendation on the Protection and Use of Health-Related Data. https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/HealthRelatedData.aspx.

Vayena E et al (2018) Policy implications of big data in the health sector. Bull World Health Organ 2018; 96:66–68. Doi: http://dx.doi.org/10.2471/BLT.17.197426.

Vayena E, Madoff L (2019) Navigating the Ethics of Big Data in Public Health. In: Mastroianni AC, Kahn JP, Kass NE (eds) The Oxford Handbook of Public Health Ethics. Doi: 10.1093/oxfordhb/9780190245191.013.31.

Vedder A et al (2014) The Law as a 'Catalyst and Facilitator' for Trust in E-Health: Challenges and Opportunities. LIT. 6(2):305-325. https://doi.org/10.5235/17579961.6.2.305.

Veil W (2020) Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt. CR-online.de Blog.CRonline Portal zum IT-Recht. 01.12.2020. Available here: https://www.cr-online.de/blog/2020/12/01/datenaltruismus-wie-die-eu-kommission-eine-gute-idee-versemmelt/

Verhenneman G, Vedder A, WITDOM, Legal and Ethical framework and privacy and security principles. Deliverable 6.1. Available here: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6%201_Legal%20and%20EthicalFrameworkand%20Privacy%20and%20Security%20Principles_v1.0_final_20150630.pdf

Wagner G in (2020) Münchener Kommentar zum BGB. 8th edition 2020. C.H. Beck München.

World Medical Association (2018) Ethical Principles for Medical Research Involving Human Subjects. Available here: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/.

The LAST-JD-RIoE project

05/04/2021

LAST-JD-RIoE-D6.6

Horizon 2020