The European Health Data Space

Examining A New Era in Data Protection

Edited by Santa Slokenberga, Katharina Ó Cathaoir and Mahsa Shabani

First published 2025

ISBN: 978-1-032-82288-4 (hbk)
ISBN: 978-1-032-89684-7 (pbk)
ISBN: 978-1-003-54411-1 (ebk)

Chapter 5

Transforming the secondary use of patient data in the European Health Data Space

A challenge for the patient's right to medical confidentiality?

Daniela Spajić

(CC-BY-NC-ND 4.0)

DOI: 10.4324/9781003544111-7

The funder of the Open Access version of this chapter is Justitierådet Edvard Cassels stiftelse, Europe Framework Programme

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

5 Transforming the secondary use of patient data in the European Health Data Space

A challenge for the patient's right to medical confidentiality?

Daniela Spajić

5.1 Introduction

Health data collected during healthcare provision is essential for advancing medical research and public health.[1] In particular, it is crucial for developing new medicines and improving personalised treatment.[2] Yet, this data – collected in a patient's medical records – contains sensitive information about the individual's health.

Historically, and also under modern human rights frameworks, patients' medical information has been subject to medical confidentiality. At the core of this principle is the unique relationship of trust between the patient and the medical professional, which encompasses an ethical dimension. It allows medical professionals to share data with others without patient consent exceptionally for reasons that are, for instance, in the public interest or serve patient safety.[3] The healthcare professional's duty of confidentiality ensures that the use of such data is restricted to the limitations of the treatment contract between patients and healthcare providers.[4]

In the EU, exceptions to patient confidentiality are laid down at multiple levels. The General Data Protection Regulation (GDPR) balances an individual's right to data protection and privacy with the collective interest in the (re-) use of personal data. Currently however, the specifics of access to patient data for different purposes are largely regulated at the national level. Regarding the sharing of patient data, some domestic legal frameworks reflect the balance between maintaining an individual's right to privacy and the objective of providing quality care by differentiating between sharing information with other care professionals to ensure quality care and the disclosure to other third-party actors.[5] The Council of Europe Recommendation also integrates such a differentiation. It urges that controllers and processors who are not health professionals should only process health-related data according to rules of confidentiality and security measures that ensure a level of protection equivalent to the one imposed on health professionals.[6]

The recently adopted European Health Data Space Regulation[7] (EHDS) seeks to transform the health data sharing regime as it implements rules that facilitate the secondary use of electronic health record data, which includes

DOI: 10.4324/9781003544111-7
This chapter has been made available under a CC BY-NC-ND 4.0 license.

patient data concerning health and genetic data in an electronic form, for various purposes. By providing specific rules for the use of such data at European Union (EU) level, the EU legislature shifts the focus from national to EU law, thereby transforming the legislative landscape to enable the sharing of patient data within and across member states.

Existing analyses have given little attention to the implications of the European Health Data Space for the physician's obligation to confidentiality. Understanding the balance between confidentiality and data protection law is an essential cornerstone of the protection of patient data, since sensitive pieces of information can provide pivotal insights into a person's health status.

The objective of this chapter is to scrutinise the rules of the EHDS concerning the secondary use of patients' electronic health record data (EHRD) from the perspective of medical confidentiality. The chapter first introduces the concept of medical confidentiality to illustrate its overarching significance in healthcare. Next, pertinent jurisprudence decided by the European Court of Human Rights (ECtHR) on the confidentiality of health data will be discussed. Afterwards, the author analyses selected provisions of the GDPR and the EHDS which relate to the secondary use of electronic health record data and confidentiality. This chapter argues that further specification within the legislative text through the EU legislature would have been needed to offer adequate protection to patients without diminishing their right to medical confidentiality.

5.2 The concept of medical confidentiality

Medical confidentiality is a keystone in medical ethics. The duty of medical professionals to maintain confidentiality guarantees the protection of patient information collected by and shared with medical professionals in the course of the patient's treatment, even after the patient's death.[8] Patients ought to speak freely about their mental and physical condition with their doctor, which in turn ought to enable healthcare professionals to make correct diagnoses and identify adequate treatments for their patients.

Although it can also extend to other healthcare professionals, the duty to preserve medical confidentiality is grounded in the Hippocratic Oath, which is historically binding on physicians. Confidentiality is sometimes enshrined in domestic law (for example, in general[9] or healthcare-related[10] frameworks). If breached without justification, this can result in disciplinary proceedings or sanctions under penal or civil law.[11]

The European Regional Office of the World Health Organisation published a notable set of principles regarding the rights of patients in Europe in 1994, including an articulation of what confidentiality and privacy ought to constitute.[12] Specifically, Article 4 of the declaration states that all 'information about a patient's health status, medical condition, diagnosis, prognosis and treatment and all other information of a personal kind must be kept confidential, even after death'. Such confidential information may 'only be disclosed if the patient gives explicit consent or if the law expressly provides for this'. The Oviedo Convention,

which aims to protect the dignity and identity of human beings with regard to the application of biology and medicine, incorporates the right to respect for private life, hence confidentiality, concerning information about one's health.[13] As similar formulations have found their way into domestic texts codifying patient rights,[14] it becomes evident that the physician's obligation to maintain patient confidentiality constitutes not only a duty of physicians and other care professionals but also a right of patients.[15] Even the sharing of patient data among medical professionals can be subject to limitations, which vary among member states.[16]

The way that patient information is managed has changed over the past decades. Patient information is not merely about what the doctor knows. It is stored in various locations such as medical records or registries, facilitating potential disclosure through access to these files.

5.3 Confidentiality and its interaction with data protection law regarding the secondary use of health data in healthcare

In this section, relevant case law of the European Court of Human Rights will be presented and elaborated upon in order to demonstrate the jurisprudential and doctrinal development of confidentiality of health data. The section then discusses patient confidentiality under the GDPR. The analysis builds the basis for the later investigation of the secondary use of health data in the EHDS.

5.3.1 Confidentiality as per the European Court of Human Rights: a vital principle, but not an absolute right

At the European regional level, Article 8 of the European Convention on Human Rights (ECHR),[17] guaranteeing the right to respect for private and family life, home and correspondence, protects the right to confidentiality of medical data. While the right to respect for one's private life is broader in scope, confidentiality forms part thereof, imposing limitations on the disclosure of information.[18] However, medical confidentiality is not an absolute right, and the patient's interest in confidentiality can be overruled where it conflicts with a competing interest, such as the re-use of patient data for public health purposes. As per Article 8(2) ECHR, there shall be no interference by a public authority with the exercise of this right unless in accordance with the law and necessary in a democratic society, taking into account the interests listed in Article 8(2) of the Convention.

5.3.1.1 Confidentiality as an aspect of the right to respect for private life

The ECtHR has assessed the relevance of the confidentiality of health data in various cases. In particular, *Z v Finland*[19] delivers a significant decision where the Court assessed the applicant's objection to the use of her medical data (encompassing information about the applicant's HIV infection) during the proceedings of a criminal court.

The Court determined that respecting the confidentiality of health data is a 'vital principle' in light of this fundamental right and thus must be respected by all contracting parties to the Convention.[20] The importance of the case is that it presents the twofold objective of medical confidentiality. Maintaining confidentiality of patient data addresses privacy concerns that arise for the patient through the disclosure of such sensitive information about their health. Furthermore, protecting patients' privacy enables patients to control who can access their data and maintains their trust and confidence in the medical profession and the provision of healthcare.[21]

Diminished confidence in the healthcare system bears various risks. Individuals could be reluctant to visit their physician, which would adversely impact their health. Also, this carries further-reaching implications that can harm community interests in preventing the spread of community diseases or a pandemic. Consequently, the Court concluded that maintaining trust in confidentiality will 'weigh heavily' in the balancing exercise. The ECtHR shows special consideration for the protection of the confidentiality of health data such as information about an individual's HIV infection, requiring 'careful scrutiny' by the court and 'the safeguards designed to secure an effective protection'. Thus, it is pivotal that domestic law safeguards patient confidentiality and discourages any disclosure of personal data to the public unless a public interest is present.[22]

5.3.1.2 Interference in accordance with the law and necessary in a democratic society

According to the jurisprudence of the European Court of Human Rights, the storing and using of personal data can already constitute an interference[23] with an individual's right to respect for private life as per Article 8(1) of the Convention. Nonetheless, such an interference can be justified according to paragraph two, provided the interference is in accordance with the law and necessary in a democratic society for one of the reasons enumerated in Article 8(2) of the Convention.

According to the majority view of the European Court of Human Rights, information about a person's medical history and treatment may be disclosed to the public under certain circumstances if the law justifies it.[24] Notably, some voices have questioned the relationship between the duty of medical confidentiality and data protection law, in particular, whether data protection legislation can take precedence over the duties of the medical professional to safeguard confidentiality and, hence, exempt the professional from the prohibition to share data concerning health without the patient's consent.[25] Similarly, according to the partly dissenting opinion of Judge de Mayer in *Z v Finland*,[26] medical confidentiality is not merely a matter of national discretion, but a human right that does not embed a margin of appreciation, and is thus to be respected by all member states. Furthermore, the dissenting opinion suggests that disclosing patient data must be subject to high standards, which not every public interest fulfils.

Even if domestic law allows access to and collection of medical data by public authorities, *LH v Latvia*[27] illustrates that it is not sufficient if the competence of the public authority is described in a general manner. In the case, a national body inspected and evaluated the medical treatment that the applicant received in a public hospital based on the applicant's medical files obtained from three different institutions. For conducting this inquiry, the national law transposed a legal basis.

The European Court of Human Rights indicated that the law must be formulated with sufficient precision and provide adequate safeguards against arbitrariness in order to be compatible with the rule of law.[28] In the case at hand, the domestic law did not limit the scope of the data that could be collected by the public authorities, which led the public authority to collect medical data about the applicant for seven years without assessing whether the data was 'potentially decisive', 'relevant' or 'important'[29] for achieving the aim of the public authority. As the inquiry by the public authority commenced seven years after the applicant's sterilisation, it was doubted whether the data was even 'necessary for purposes of medical treatment [or] provision or administration of health care services' in accordance with the national law. In light of these considerations, it became less relevant for the court whether the staff of the public authority itself had a legal duty to maintain confidentiality.[30] Consequently, the court held that the domestic law was not sufficiently precisely formulated. Furthermore, the scope of discretion by the public authority and the manner of its exercise were not sufficiently specified.[31]

As indicated above, Article 8(2) of the European Convention on Human Rights lists concrete interests that can be balanced against an individual's interest in his or her right to private life, namely interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. Interestingly, however, the Oviedo Convention[32] did not consider all exceptions listed in Article 8(2) of the European Convention on Human Rights as relevant. The reason being was that it did not appear desirable to make the protection of a person's rights in the health sphere subject to defending the economic well-being of the country,[33] public order or morals, and national security.[34]

Finally, unavoidable interference should be limited to the extent that it is strictly necessary in a democratic society.[35] According to the European Court of Human Rights, the notion of necessity within the meaning of Article 8 of the Convention implies the existence of a 'pressing social need' and, in particular, that the measure is proportionate to the legitimate aim.[36] Thus, the notion of 'public interest' has to meet the high threshold of a 'pressing social need' which could encompass for instance travel restrictions as a potential public health measure where a risk of the spread of highly contagious diseases exists.[37] What constitutes a 'pressing social need' and how the principle of confidentiality is to be applied is, according to the Court, a decision that remains with the contracting countries as it is in their 'margin of appreciation'.[38]

5.3.2 The concept of medical confidentiality under the GDPR

Moving to the GDPR, the Regulation seeks to balance the (re-)use of patient data for the improvement of healthcare, research and public health with the patient's right to data protection and (medical) privacy.[39] Consequently, for data holders to share personal electronic healthcare record data (EHRD) with health data access bodies as foreseen by the EHDS, they need to comply with the rules of the GDPR in addition to those set out in the EHDS.

According to the GDPR, the processing of data concerning health and genetic data as a special category of personal data is generally prohibited as per Article 9(1) GDPR. In contrast, Article 9(2) GDPR exempts this prohibition, thereby legitimising the processing of data concerning health in conjunction with an adequate legal basis laid down in Article 6 GDPR. Data controllers must choose an adequate legal basis for the processing of these data types, whereby none of the legal grounds receives precedence over the other.

The GDPR uses the notion of professional secrecy where the medical confidentiality of patient data is concerned. For healthcare purposes, the GDPR incorporates a provision with Article 9(2)(h) GDPR that is tailored to the need for processing patient data. Specifically, it enables processing of special categories of personal data such as data concerning health and genetic data for purposes of preventive or occupational medicine, medical diagnosis, or the provision of health or social care more generally on the basis of Union or national law or pursuant to contract with health professionals and subject to the conditions and safeguards as per Article 9(3) GDPR.[40] The latter in particular requires that special categories of personal data are processed by or under the responsibility of a professional who is subject to the obligation of professional secrecy. Other persons may also process personal data as long as they are subject to an obligation of secrecy.[41] From this provision, it becomes evident that the GDPR uses the notion of professional secrecy where the medical confidentiality of patient data is concerned.

Additionally, although it does not provide a specific definition for the term, the GDPR has also embedded the concept of 'confidentiality' as one of its principles applicable to the processing of personal data, namely the principle of integrity and confidentiality.[42] This principle requires data controllers and processors to process personal data in a manner 'that ensures appropriate security of personal data'. This includes the obligation to implement appropriate technical and organisational safeguards for protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using technical or organisational measures.[43] By doing so, the GDPR positions the term 'confidentiality' mainly in relation to the security of the processing operations.[44] It also does so in terms of other relevant provisions of the GDPR, such as in Articles 28[45] and 32 GDPR.[46] Similarly, the European Data Protection Board (EDPB) specifies the role of the principle of integrity and confidentiality, considering it as a means to avoid data breaches and to ensure compliance with the rules and principles concerning data processing under the GDPR, thereby also

assuring compliance with the data protection by design and by default principles.[47] Implementing security is, as the EDPB stresses, an ongoing process that requires continuous assessment of the measures in place and their appropriateness to address technical threats or weaknesses.[48]

The deployment of appropriate technical and organisational measures is pivotal, particularly for protecting the rights and freedoms of natural persons, as Recital 78 GDPR highlights. In addition to putting adequate information systems in place (such as the technical means to manage access control and enable secure data transfers),[49] against that background, the principle of data minimisation[50] can be considered another component or facilitator for securing data confidentiality by limiting personal data collection and data usage to the absolute minimum.[51] The process of pseudonymising[52] or anonymising personal data can be a safeguard that maintains data confidentiality and secures the data subject's identity. Anonymisation as such is a further processing of personal data and, thus, must fulfil the compatibility clause as per Article 5(1)(b) GDPR taking account of the circumstances of said further processing.[53] Yet, note should be taken that the compatibility clause may not be applicable where data concerning health is collected during the provision of healthcare for research purposes if national law does not account for both purposes.[54]

5.4 Patient data under the secondary use framework of the European Health Data Space

The EHDS transposes a framework for secondary use that is defined as the processing of electronic health data (EHD) for purposes (set out in Chapter IV of the Regulation) other than the initial purposes for which they were collected or produced.[55]

EHRD will be collected by default, whereby individuals have the right to opt-out from the processing of their data for secondary use at any time.[56] Member states shall transpose mechanisms to implement the right to opt-out at the national level. The right to opt-out will be limited as member states may establish rules in national law transposing exceptions for certain purposes,[57] namely for the public interest in the area of public and occupational health (Articles 71(4)(a)(i) and 53(1)(a) EHDS), policy making and regulatory activities (Articles 71(4)(a)(i) and 53(1)(b) EHDS), statistics (Articles 71(4)(a)(i) and 53(1)(c) EHDS), and, finally, scientific research for important reasons of public interest (Article 71(4)(a)(ii) EHDS).[58] Access to data for these purposes shall be reserved for public sector and Union bodies, as well as third parties who carry out a task on their behalf.[59]

While EU member states may transpose further categories of EHD for secondary use,[60] Article 51 EHDS enumerates the minimum categories of EHD, which includes data from electronic health records (EHRs).[61] Nonetheless, other data categories that are listed in Article 51 EHDS may also be collected during the patient's treatment such as data on factors impacting on health (for example, socio-economic, environmental, and behavioural factors), automatically generated

personal EHD through medical devices, or human genetic, epigenomic and genomic data.[62] All these categories of data are typically collected in the healthcare system, which is an environment significantly shaped by trust and confidentiality,[63] which the EHDS fails to consider.

The reuse of the enumerated categories will be possible for an array of purposes. Chapter IV of the EHDS provides a list of grounds based on which it should be possible to process EHD for secondary use, including purposes such as public interest in the area of public and occupational health,[64] education or teaching activities in the health or care sector at the level of vocational or higher education,[65] or scientific research related to health or care sectors, contributing to public health or health technology assessment or ensuring high levels of quality and safety of health care, of medicinal products or medical devices.[66] These have been embedded in the EHDS (presumably) in accordance with the corresponding legal grounds laid down in the GDPR (i.e., Articles 9(2)(g, h, i and j) GDPR).[67] The challenges that may arise from the interaction between the EHDS and the GDPR – particularly with a view to these provisions – will be elaborated later in this chapter.

Article 54 stipulates that health data users shall process EHD for secondary use only in compliance with the data permit and data request as per Articles 68 and 69 EHDS, respectively. Considering the sensitivity of EHD, and in particular EHRs, the EU legislature integrated a list of prohibited secondary uses of EHD, including a prohibition for advertising or marketing activities or for taking decisions detrimental to a natural person or a group of natural persons based on their EHD or in relation to a job offer.[68]

To foster access to health data for secondary use, the EHDS foresees the establishment of so-called health data access bodies, which will be responsible for granting access to EHD and which are further discussed in Chapters 9 and 10.[69] Data holders will have to make various categories of EHD available to health data access bodies, as the framework establishes a duty in the sense of Article 6(1)(c) GDPR for them to share EHD with health data access bodies[70] for secondary use.[71] While the original proposal put forward by the Commission considered such a duty for 'data holders',[72] the compromise text speaks of '*health* data holders'.[73] Although the amendment to the concept of health data holder and its corresponding definition suggests a clearer delineation as to whom the obligation to share health data applies, it still encompasses a wide range of stakeholders. This is because, according to the EHDS, a health data holder is a natural and legal person, public authority, agency or other body in the healthcare or the care sector as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to healthcare or care sectors, or acting as a mortality registry as well as Union institutions, body, office or agency.[74]

Following a successful permit request for data access, health data access bodies will issue a permit in a subsequent step and offer access to EHD in an anonymised format to data users.[75] Similar to the definition of the health

data holder, the final text speaks now of 'health data users' while still providing a broad definition for this concept, covering a natural or legal person that has been granted lawful access to EHD for secondary use pursuant to a data permit, data request or an access approval by an authorised participant in HealthData@EU.[76] Notably, the text of the EHDS did not adopt the suggestion put forward by the European Parliament to restrict data access to health data applicants who have a demonstratable professional link to the areas of health care, public health or medical research and that submit an application for health data.[77] By neglecting to do so, the final text again expands its scope of application to all kinds of data users with and without a professional link to the medical field, including commercial players, raising potential challenges for the patient's right to confidentiality (see further in Chapter 8).

Though health data users should primarily be granted access to anonymised data, the EHDS does not entirely exclude the sharing of personal data. Access to pseudonymous data,[78] hence personal data, can be granted where the data user cannot fulfil the anticipated purpose with anonymised data.[79] In such cases, data users will have to demonstrate how the data processing complies with the GDPR, in particular regarding the legal basis as per Article 6(1) GDPR on which they rely for the secondary use of EHD as part of the data access application.[80] Thereby, the compromise text fails to create harmonisation with the secondary use of personal EHD under the EHDS, especially as the identification of a legal basis as per GDPR is required.

5.5 Potential challenges arising between the EHDS, ECtHR case law and GDPR with regard to the secondary use of patient data

The above overview of relevant jurisprudence of the European Court of Human Rights and provisions of the GDPR and EHDS provided insights into the legal requirements of (patient) confidentiality, and how certain public interests can outweigh a patient's interest in confidentiality. The following analysis will elaborate on these perspectives in relation to the secondary use framework under the European Health Data Space.

The Regulation foresees that health data holders should be able to rely on the legal grounds of Article 6(1) GDPR, i.e., a (consent), c (compliance with a legal obligation), e (public interest) or f (legitimate interest), in conjunction with Article 9(2) GDPR, i.e., g (substantial public interest), h (preventive or occupational medicine), i (public interest in the area of public health) or j (archiving purposes in the public interest, scientific research or statistical purposes), when sharing personal health data with health data access bodies.[81] The following section thus investigates the challenges that the new framework carries for patient confidentiality, namely the need for legal specification of the patient's right to confidentiality and the need to improve the delineation of the purposes laid down in Article 53 EHDS with regard to Article 9 GDPR.

5.5.1 Article 9(2)(h) in conjunction with Article 9(3) GDPR

Neither the Proposal nor the latest EHDS text have specified how the grounds set out in the GDPR and the EHDS are compatible.[82] This question persists in particular concerning Article 9(2)(h), as it integrates an exception to the prohibition tailored to the processing of data concerning health for the provision of care. This provision enables the use of patient data for various types of medical care such as diagnosis or health prevention. Further processing that is not necessary for the provision and management of healthcare services, such as medical research, is not covered by the provision.[83]

Article 9(2)(h) has to be read in conjunction with Article 9(3) GDPR, and therefore, the latter's conditions must also be fulfilled in order for the exception of paragraph (h) to apply. Article 9(3) GDPR requires that special categories of personal data can be

> "processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

Given that such obligations of professional secrecy are usually embedded in national legislation, the fulfilment of the requirements of Article 9(3) GDPR – and consequently also the fulfilment of the conditions laid down in Article 9(2)(h) GDPR – will depend on domestic legislation.[84]

In relation to Article 8(3) of the EU Data Protection Directive,[85] which constitutes the preceding equivalent to what is now Article 9(2)(h) GDPR, the Article 29 Data Protection Working Party (hereafter WP29) concluded that all patients may 'reasonably expect that confidentiality and protection of their personal information will be rigorously upheld by all healthcare professionals', also 'as regards electronic health record (EHR) systems'.[86] Data collected under Article 8(3) Data Protection Directive had thus to be interpreted in a restrictive way. Subsequently, Article 8(3) could only serve as a legal ground to the extent that such data were processed strictly for medical and healthcare purposes and were required to be processed by a health professional.[87]

Given the restricted scope of Article 9(3) GDPR, the obligations established under data protection law appear to collide with the obligation to share data with health data access bodies. This constitutes an issue for healthcare professionals, since, as the WP29 pointed out, the obligation of professional secrecy must be established by law or by professional bodies through binding rules at national level.[88] In other words, does Article 9(2)(h) GDPR constitute an adequate legal basis for healthcare professionals when providing care to their patients while having to share the data further with health data access bodies as foreseen under the EHDS, or will this provision become obsolete once the EHDS is transposed? The question persists as the EDPB held in its opinion

from 2021 that the presumption of compatibility as per Article 5(1)(b) GDPR cannot be upheld in terms of the further sharing of patient data for scientific research purposes unless national legislation stipulates otherwise.[89]

Certain categories of health data holders, namely natural persons, individual researchers and legal persons that are micro-enterprises, should be exempted from the obligations on the secondary use as per Article 50 EHDS. However, member states may provide that the obligations apply to them under national legislation.[90] Also, health data intermediation entities may support health data holders to fulfil their duties if domestic law provides for it,[91] although the relationship between healthcare professionals and health data intermediation entities may require further clarification.[92]

This prompts the subsequent question of whether healthcare providers will need to rely on explicit consent in order to respect their legal obligation to share data with health data access bodies. The European Parliament originally required that the patient's explicit consent (opt-in) should be requested for the secondary use of certain sensitive data, such as genetic data.[93] The EHDS transposes instead a right to opt-out, which member states ought to facilitate, leaving it within their competence to offer an absolute right to object to access related to specific categories of personal EHD, such as genetic data (see further in Chapter 7).[94]

Meanwhile, the so-called data altruism consent established under the Data Governance Act (DGA) may be a useful tool in addressing this concern (see further in Chapter 6). The EHDS foresees fostering altruistic data sharing based on the data altruism consent. However, legal uncertainty is created through the lack of clarity regarding the interplay between the EHDS, the GDPR and the DGA.[95] The latter has established particular rules to foster data sharing for the public good through the data altruism consent form. Data altruism encompasses objectives of general interest as provided for in national law,[96] such as (but not limited to) healthcare.[97] By doing so, the data altruism consent established under the DGA gives the impression that this form of consent is broader in scope compared to the 'common' GDPR consent which orients itself more strictly after the purpose limitation principle. Legal uncertainties remain given that as per Recital 50 DGA, data altruism consent will rely on the meaning of consent as established under the GDPR. Thus, the lack of alignment between the provisions of the GDPR and the DGA is carried into the scope of the EHDS. Furthermore, the vague definition of data altruism potentially extends access to protected patient data a little further by including stakeholders who do not demonstrate a professional link to healthcare.

The adaptations which had been suggested by the European Parliament in December 2023 appeared to address this issue to the extent that access would have been restricted to 'health data applicants', who are 'any natural or legal person with a demonstratable professional link to the areas of health care, public health or medical research and that submits an application for health data'.[98] However, this definition has not been integrated into the final text. Instead, considerations regarding the need to respect professional duties

such as confidentiality duties have been integrated into the recitals. More specifically, according to Recital 55 of the EHDS, health data holders (such as healthcare providers) should make different categories of EHD available for secondary use 'provided that such effort is always made through effective and secured processes, with due respect for professional duties, such as confidentiality duties'. Although recitals represent the legislature's will and are hence needed for the interpretation of the law, they are not directly binding. Thus, also considering the case law of the European Court of Human Rights requiring the implementation of safeguards and legal specificity, a provision dedicated to professional duties and patient confidentiality should have been adopted.[99]

Besides, Recital 55 addresses only the sharing of health data through health data holders while the need to address confidentiality concerns with regard to health data *users*, who are not subject to such professional duties, persists. Even though the EHDS focuses on the sharing of anonymous data, this concern exists as the sharing of anonymous EHD facilitated through the European Health Data Space bears the risk to lead to centralised data silos carrying with them privacy and security concerns.[100]

Eliminating the risk of re-identification has proven to be difficult in practice, particularly in the context of healthcare.[101] Especially in terms of genetic data, which should also be integrated into the European health data space as a data category,[102] anonymisation seems to be unattainable according to the current technological state of the art.[103] Certain categories of health data, such as health data collected from patients with rare diseases, which occur in not more than five in ten thousand persons, carry a risk for individuals to be re-identified even when state-of-the-art anonymisation techniques have been applied, as the combination of information or vastly evolving technological developments can reveal sensitive information. The legislature acknowledges that a risk of re-identification remains regarding such data types. According to Recital 92 EHDS, this falls within the criteria of Article 5(13) DGA, which allows the European Commission to adopt delegated acts to lay down requirements for data transfer to third countries.[104] As the provision focuses on data transfers to third countries, interestingly, the legislature seems to suggest that a risk of re-identification for such data types does not exist within the European Union.[105]

5.5.2 Articles 9(2)(i) and (j) GDPR

While the purposes for secondary use were much broader defined in the Proposal, the European Parliament suggested narrowing the scope of application of secondary use. In particular, secondary use in, for instance, the labour market or financial services was to be banned, given that the data shared for research purposes should foster the improvement of medicine and healthcare services and products.[106] This certainly aligns better with the notions of public interest in the area of public health and scientific research as per Articles 9(2)(i) and (j) GDPR, respectively.

According to the EHDS, individuals will be able to exercise the opt-out mechanism without having to provide any reason for their decision. However, patients will not be able to opt-out for purposes that have a strong link to the public interest.[107] Recital 54 EHDS exemplifies some purposes which constitute a strong link to the public interest, such as activities for protection against serious cross-border threats to health or scientific research for important reasons of public interest, including, for instance, research addressing medical needs (such as rare diseases or emerging health threats). These purposes align in parts with the case law illustrated earlier in this chapter.

However, what can constitute a reason that is in the public interest and is necessary to pursue, meaning fulfilling a 'pressing social need',[108] and how the principle of confidentiality is to be applied is, returning to the jurisprudence of the European Court of Human Rights, a decision that remains with the contracting countries as it is within their 'margin of appreciation'.[109] Exceptions to the healthcare provider's duty of confidentiality can, thus, be found in national laws. The transposition of these laws can deviate between countries. For instance, some countries enable the use of EHR data for secondary purposes based on data protection legislation, while others implement specific legislation for it,[110] or they may transpose provisions supporting data transfer to specific registries.[111]

While acknowledging that some of these notions comprise altruistic purposes,[112] meaning purposes which serve broader societal interests such as the improvement of healthcare services, they have created legal uncertainty due to a deficient definition.[113] This may be partly due to the fact that member states conceptualise the notion of public interest or scientific research differently, leading to fragmented approaches to research and public health interests among EU member states.

For instance, if interpreted in the strict sense, the public interest may encompass purely public purposes such as public health, thereby excluding the full or partial involvement of commercial companies.[114] In such circumstances, sharing health data with the latter could lead to a violation of patient confidentiality, which the Proposal did not seem to consider sufficiently.[115] In contrast, the EHDS, as mentioned earlier, reserves explicitly the use of EHD for public interest to public sector bodies. However, it does again not account for professional secrecy although Article 9(2)(i) GDPR explicitly requires the implementation of suitable and specific measures to safeguard the rights and freedoms of individuals, in particular in relation to professional secrecy.

Furthermore, a clearer alignment by the legislature of the purposes listed in Article 53 EHDS by delineating still ambiguous notions, such as scientific research (Article 9(2)(j) GDPR), would have been needed to safeguard patient confidentiality. This is because the concept of scientific research can be associated with two different legal grounds in the EHDS, i.e., 'public interest' (Article 53(1)(a) EHDS) and 'scientific research related to health and care' (Article 53(1)(e) EHDS). Especially regarding the former, scientific research may constitute a 'public interest' as per Article 53(1)(a) EHDS if conducted for an

important reason in the public interest according to Recital 54 EHDS. However, it is yet to be seen how both legal grounds (i.e., paragraphs a) and e)) will be applied. A possibility to address this issue can be to link the purposes more explicitly to the exceptions laid out in Article 9(2) GDPR[116] given that Article 9(2)(i) GDPR specifies that it applies to the protection 'against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices'.

Finally, while complete datasets may be admirable to achieve, the unlimited collection and storage of personal EHD for the secondary use should be avoided in light of ECtHR case law. In particular, the collection and sharing of medical data should be assessed in terms of its 'relevance' or 'importance' to understand whether the data is (still) necessary for the purpose for which it was collected in order to ensure compatibility with the rule of law.

5.5.3 Article 9(4) GDPR

The question of the legality of the processing of sensitive patient data in the European Health Data Space with a view to the physician's duty of medical confidentiality remains, especially also in light of Article 9(4) GDPR. This provision allows member states to introduce further requirements, including limitations on the processing of data concerning health, biometric data and genetic data. These have led to varying levels of digitalisation of health data depending on data categories.[117] While the legislature constructs the EHDS as an EU law that addresses the fragmented implementation created by Article 9(4) GDPR,[118] it remains somewhat unclear how the EHDS plans to conform with this provision.[119] Notably, the EHDS explains that member states may no longer make use of paragraph 4 to transpose further conditions, including limitations and specific provisions requesting consent of individuals, regarding secondary use, except as referred to in Article 51(4) EHDS.[120] This has prompted the question of if and how the margin of appreciation per Article 9(4) GDPR can be sustained.

5.6 Conclusion

The analysis in this chapter shows that the EHDS is not fully harmonised with the existing rules of the GDPR. Above all, the forthcoming legislative changes initiated to foster the secondary use of health data appear to challenge patient confidentiality.

Deontological rules of confidentiality primarily concern healthcare professionals and their obligations rather than those who seek to process patient data. Breach of such duty would thus primarily concern healthcare professionals if punishable under domestic law. More importantly, however, these rules exist for the protection of the patient, making the duty of medical professionals a patients' right. The European Parliament's propositions following their reading in December 2023 considered this concern to a certain degree and thus

would have gone in the right direction. Integrating the duty to patient confidentiality into the provisions, not only with a view to data holders but also with a view to data users, contributes to avoiding potential disharmony with the patient's right to confidentiality.

Finally, it should be considered that healthcare is primarily a matter of national competence, which complicates the re-use of patient data and does not seem to be taken sufficiently into consideration by the EHDS. This may lead to a collision between the patient's interest in medical confidentiality and the EHDS's interest in fostering the availability of EHR data. Also, attention must be paid to the fact that the patient–doctor relationship is characterised by a special bond of trust, creating high standards for the potential re-use and sharing of sensitive data. Otherwise, this could impede patients from receiving suitable healthcare. To this end, the jurisprudence by the European Court of Human Rights provides some guidance that could shape the implementation of the European health data space and its Regulation.

Acknowledgement

The research for this chapter was in part performed in a project that received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101095717. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Notes

1 Commission, 'A European strategy for data' (Communication) COM/2020/66 final.
2 Data Saves Lives, 'Why is health data important?' www.datasaveslives.eu/why-is-health-data-important accessed 28 April 2024; MedTech Europe, 'Unlocking the full benefits of health data. Recommendations from MedTech Europe' (2021) position paper 16 June 2021 www.medtecheurope.org/wp-content/uploads/2021/06/mte_160621_positionpaper_health-data.pdf accessed 28 April 2024.
3 Henriette Roscam Abbing, 'Medical Confidentiality and Patient Safety: Reporting Procedures' (2014) 21(3) *European Journal of Health Law* 245.
4 Article 29 Working Party (WP29), 'Working Document on the processing of personal data relating to health in electronic health records (EHR)' (WP 131, 15 February 2007) 10.
5 See Mette Hartlev, 'Forwards or backwards? New directions in Danish patients' Rights Legislation' (2011) 18(4) *European Journal of Health Law* 365, 371, according to which such differentiation can be found in the Danish Health Act (see Chapter 9 of the Danish Health Act (S*undhedsloven LBK nr 247 of 12 March 2024* (Denmark)); another example is § 9 of the (Model-)Professional Code for Physicians in Germany (*(Muster-) Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte MBO-Ä 1997*) (Germany).
6 Council of Europe, 'Protection of health-related data' Recommendation CM/Rec(2019)2, 2 March 2019. See Article 9.4, which stipulates similar obligations for the communication of health-related data to an authorised recipient for purposes other than providing and administering health care.

7 European Parliament, 'CORRIGENDUM to the position of the European Parliament adopted at first reading on 24 April 2024 with a view to the adoption of Regulation (EU) 2024/… of the European Parliament and of the Council on the European Health Data Space' P9_TA(2024)0331 (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), 27.11.2024 (hereafter EHDS).

8 See, for instance, World Medical Association (WMA), 'Declaration of Lisbon on the rights of the patient' (1981) www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/ accessed 28 April 2024, art 8(a).

9 See, for instance, Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslag* (2009:400)) (Sweden).

10 See, for instance, (Model-)Professional Code for Physicians in Germany (n 5). The duty of confidentiality may be specified in soft law (see, for instance: Medical Council, 'Guide to Professional Conduct and Ethics for Registered Medical Practitioners (Amended)' (2016) last updated 2019, 25 (Ireland) www.medicalcouncil.ie/news-and-publications/reports/guide-to-professional-conduct-ethics-8th-edition.html accessed 28 April 2024).

11 For instance, Germany regulates the penalties for the breach of medical secrecy in section 203 of the German Criminal Code (*Strafgesetzbuch*) in conjunction with the (Model-)Professional Code for Physicians in Germany (n 5).

12 Abbing (n 3); The duty is also embedded in other instruments at international level, in particular in the Declaration of Geneva which is considered to be the 'modern Hippocratic oath' (see WMA, 'Declaration of Geneva' (1948) www.wma.net/policies-post/wma-declaration-of-geneva/ accessed 28 April 2024; or WMA, 'Declaration of Geneva, The 'Modern Hippocratic Oath' www.wma.net/what-we-do/medical-ethics/declaration-of-geneva/ accessed 28 April 2024; Other international instruments are, for instance: WMA, 'Declaration of Lisbon on the rights of the patient' www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/ accessed 28 April 2024, or 'WMA International Code of Medical Ethics' www.wma.net/policies-post/wma-international-code-of-medical-ethics/ accessed 28 April 2024.

13 Council of Europe, 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 CETS no 164 (Oviedo Convention) art 10; see also: Council of Europe, Explanatory report to the Convention on Human Rights and Biomedicine, para 63, 10, www.coe.int/en/web/bioethics/oviedo-convention accessed 28 April 2024.

14 See, for example, § 9 of (Model-)Professional Code for Physicians in Germany (n 5); or § 54 of Federal Physicians Act (*Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte (Ärztegesetz 1998 – ÄrzteG 1998*), StF: Federal Law Gazette I Nr. 169/1998 (Austria).

15 Abbing (n 3).

16 See legislation (n 9-10).

17 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols no 11, 14 and 15, supplemented by Protocols no 1, 4, 6, 7, 12, 13 and 16) 4 November 1950, ETS 5 (hereinafter also referred to as the Convention/ECHR).

18 Maria Sokalska, 'Medical confidentiality – Quo Vadis?' (2004) 11(1) *European Journal of Health Law* 35; Oviedo Convention, art 10 (n 13). The right has been reiterated in Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data CETS No 108 (2018) (Convention 108+)); also, the Council of Europe's recommendation on the protection of health-related data (see above (n 6)) takes account of the concept of patient confidentiality.

19 *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997).

20 *Z v Finland* (n 19) para 94.

21 *Z v Finland* (n 19) para 95.
22 *Armonas v Lithuania* App no 36919/02 (ECtHR, 25 November 2008) para 40; *Biriuk v Lithuania* App no 23373/03 (ECtHR, 25 November 2008) paras 43-44; *Z v Finland* (n 19) para 95.
23 See *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987) para 48; *S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008); *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000).
24 See, for instance, *Panteleyenko v Ukraine* App no 11901/02 (ECtHR, 29 June 2006).
25 See Christian Katzenmeier, 'Berufsgeheimnis und Dokumentation' in Adolf Laufs, Christian Katzenmeier and Volker Lipp (eds), *Arztrecht* (Verlag CH Beck oHG 2021) para 79.
26 *Z v Finland* (n 19).
27 *LH v Latvia* App no 52019/07 (ECtHR, 29 April 2014).
28 *LH v Latvia (n 27)* para 47.
29 See *LH v Latvia (n 27)* para 58, referring to *LL v France* App no 7508/02 (ECtHR, 10 October 2006) para 46, and *MS v Sweden* App no 20837/92 (ECtHR, 27 August 1997) paras 38, 42 and 43.
30 *LH v Latvia* (n 27) para 58.
31 *LH v Latvia (n 27)* para 59.
32 Oviedo Convention (n 13).
33 The economic aspect is taken into account insofar as Article 3 of the Convention refers to 'available resources'. This, however, should not be a reason for allowing exceptions to the rights established under the Convention (see Explanatory Report (n 13) paras 157 and 159, at 22; Abbing (n 3) 248–249).
34 See Explanatory Report (n 13) para 156, at 22; Article 26 of the Oviedo Convention covers interests of public safety, prevention of crime, protection of public health, protection of rights and freedoms of others as possible exceptions to medical confidentiality; see Abbing (n 3) 248–249.
35 See, for instance, *LL v France* (n 29) para 43.
36 See *Biržietis v Lithuania* App no. 49304/09 (ECtHR, 14 June 2016).
37 See *Handyside v the United Kingdom* App no 5493/72 (ECtHR, 07 December 1976); *Kiyutin v Russia* App no 2700/10 (ECtHR, 10 March 2011).
38 *Z v Finland* (n 19).
39 See, for instance, Edward S Dove, 'Confidentiality, public interest, and the human right to science: when can confidential information be used for the benefit of the wider community?' (2023) 10(1) *J Law Biosci Journal of Law and the Bioscience* lsad013.
40 See GDPR art 9(2)(h).
41 GDPR art 9(3).
42 GDPR art 5(1)(f).
43 GDPR art 5(1)(f).
44 Sometimes, the GDPR connects confidentiality to the role of a person (see art 38(5) GDPR).
45 See art 28(3)(b) GDPR which refers to confidentiality related to (un-)authorised access.
46 See art 32(1)(b) GDPR which refers to the security of processing.
47 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0' (2019) 20 *October* 2020, 26.
48 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0' (2019) 20 *October* 2020.
49 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0' (2019) 20 *October* 2020, 26–27.
50 See GDPR art 5(1)(c).
51 See GDPR rec 78.
52 See GDPR rec 78, art 4(5).

53 WP29, 'Opinion 05/2014 on Anonymisation Techniques' (WP 216, 10 April 2014).
54 EDPB, 'EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research' (2021) 2 February 2021, 6–7.
55 EHDS art 2(2)(e).
56 EHDS rec 54, art 71.
57 EHDS art 71(4)(a).
58 See also: EHDS rec 54.
59 EHDS arts 53(2), 71(4)(a).
60 EHDS art 51(2).
61 EHDS arts 51(1)(a), 2(2)(j).
62 EHDS art 51(1)(b), (f) and (h).
63 Santa Slokenberga, 'Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along' (2022) Technology and Regulation 135, 142.
64 EHDS art 53(1)(a).
65 EHDS art 53(1)(d).
66 EHDS art 53(1)(e).
67 See: EHDS rec 52, art 2(2)(a).
68 EHDS art 54(a-c).
69 EHDS art 55.
70 EHDS art 57.
71 See EDPB-EDPS, 'Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' (2022) 12 July 2022, para 22.
72 See Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM/2022/197 final (EHDS (proposal)) art 2(2)(y).
73 EHDS art 2(2)(t). Emphasis added.
74 EHDS art 2(2)(t).
75 EHDS rec 53, art 66(2).
76 EHDS art 2(2)(u).
77 See European Parliament, 'Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))(1), T9-0462/2023, Amendment 105, art 2 – paragraph 2 – point z a (new).
78 See GDPR art 4(5).
79 EHDS arts 66(3), 67(2)(e), 67(4).
80 EHDS rec 52, art 67(4).
81 EHDS rec 52.
82 EDPB-EDPS (n 71) para 89-90.
83 WP29 (n 4) 10.
84 Georgieva Ludmila, Christopher Kuner, 'Article 9 Processing of special categories of personal data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford Academic, online edn 2020).
85 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.
86 WP29 (n 4) 21.
87 WP29 (n 4) 11.
88 WP29 (n 4) 11.
89 EDPB (n 54) 7, para. 22.
90 EHDS art 50(1 and 2).

91 EHDS art 50(3).
92 Standing Committee of European Doctors (CPME), 'European doctors call for more ambition on professional secrecy and patient confidentiality in European Health Data Space', 8 February 2024, https://www.cpme.eu/news/european-doctors-call-for-more-ambition-on-professional-secrecy-and-patient-confidentiality-in-european-health-data-space accessed 28 April 2024.
93 European Parliament, 'EP supports creating EU Health Data Space to boost access to data and research' (press release, 13 December 2023) www.europarl.europa.eu/news/en/press-room/20231208IPR15783/ep-supports-creating-eu-health-data-space-to-boost-access-to-data-and-research accessed 28 April 2024; see also: European Parliament (n 77) amendment 39, recital 39 a (new).
94 EHDS rec 18; see also EHDS rec 11.
95 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) PE/85/2021/REV/, OJ L 152 [hereinafter also referred to as 'DGA'].
96 See DGA art 2(16).
97 See DGA art 2(16) for all examples constituting 'objectives of general interest'.
98 European Parliament (n 77) amendment 105, Article 2, paragraph 2, point z a (new).
99 Standing Committee of European Doctors (CPME) (n 92).
100 René Raab and others, 'Federated electronic health records for the European Health Data Space' (2023) 5(11) *Lancet Digital Health* e840.
101 See WP29 (n 53) 22, 33-34.
102 EHDS art 51(1)(f).
103 See Harald Schmidt and Shawneequa Callier, 'How anonymous is "anonymous'anonymous"? Some suggestions towards a coherent universal coding system for genetic samples' (2012) 38(5) *Journal of Medical Ethics* 304.
104 EHDS rec 92. see also DGA arts 5(13) and 32.
105 David Fåhraeus, Jane Reichel and Santa Slokenberga, 'The European Health Data Space: Challenges and Opportunities' (European Policy Analysis, Sieps – Swedish Institute for European Policy Studies, February 2024) 9–10.
106 European Parliament, 'EP supports creating EU Health Data Space to boost access to data and research' (2023) press release, 13 December 2023 www.europarl.europa.eu/news/en/press-room/20231208IPR15783/ep-supports-creating-eu-health-data-space-to-boost-access-to-data-and-research accessed 28 April 2024.
107 EHDS rec 54; EHDS 71(4).
108 See *Biržietis v Lithuania* (n 36); *Handyside v the United Kingdom* (n 37); *Kiyutin v Russia* (n 37).
109 *Z v Finland* (n 19).
110 See Time.lex and Milieu, 'Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations' (2014) 45–47 https://health.ec.europa.eu/other-pages/basic-page/overview-national-laws-electronic-health-records-eu-member-states-2016_en accessed 28 April 2024.
111 For instance, see: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), 'Register im Gesundheitsbereich' www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/Allgemein/RegisterimGesundheitsbereich.html accessed 28 April 2024.
112 Anton Vedder and Daniela Spajic, 'Moral autonomy of patients and legal barriers to a possible duty of health related data sharing' (2023) 25 *Ethics and Information Technology* 23.
113 For instance, the EDPS stresses that not every research activity can fulfil the criteria for *scientific* research (see EDPS, 'A Preliminary Opinion on data protection

and scientific research' (2020) 11–12). Also, uncertainties remain as to what public interest can be considered as *substantial* public interest as per Article 9(2)(g) GDPR (see Daniela Spajic, 'Patient data sharing for the improvement of healthcare and medical research: Towards a moral duty of patients to share health-related data?' (PhD Dissertation, KU Leuven 2023)).

114 John Mark Michael Rumbold and Barbara Pierscionek, 'The Effect of the General Data Protection Regulation on Medical Research' (2017) 19(2) *Journal of Medical Internet Research* e47, 2.

115 See EHDS (proposal) (n 72) art 2(1)(z), according to which data user is broadly defined as 'a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use'.

116 Veronique Cimina, 'The Proposal for a European Health Data Space: between pursued objectives and data protection challenges' (2023) 24 ERA Forum 343, referring to EDPB-EDPS (n 71) paras 82 to 99.

117 EHDS rec 27.

118 EHDS (proposal) (n 72) explanatory memorandum. Notably, the EHDS still considers a potential fragmentation as valid when it comes to international transfers of personal electronic health data (see EHDS art 90).

119 EDPB-EDPS (n 71) paras 57, 89.

120 See EHDS rec 52.

List of sources

Treaties, legislation and conventions

Council of Europe, 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, CETS No. 164 (Oviedo Convention).

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, CETS 108.

Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, 18 May 2018 (Convention 108+).

Council of Europe, European Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, 4 November 1950, CETS 5.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

European Parliament, 'CORRIGENDUM to the position of the European Parliament adopted at first reading on 24 April 2024 with a view to the adoption of Regulation (EU) 2024/… of the European Parliament and of the Council on the European Health Data Space' P9_TA(2024)0331 (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), 27.11.2024 (European Health Data Space Regulation - EHDS).

Proposal for a Regulation of the European Parliament and of The Council on the European Health Data Space (EHDS proposal) COM/2022/197 final.

Proposal for a Regulation of The European Parliament and of The Council on European data governance (Data Governance Act, DGA) COM/2020/767 final.

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, GDPR) OJ L 119/1.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) PE/85/2021/REV/, OJ L 152/1.

Domestic legislation

Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906) (*Strafgesetzbuch*) (Germany).

Federal Physicians Act (*Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte (Ärztegesetz 1998 – ÄrzteG 1998)*, StF: Federal Law Gazette I Nr. 169/1998 (Austria).

Health Act (consolidated) (S*undhedsloven LBK nr 247 of 12 March 2024*) (Denmark).

Medical Council, 'Guide to Professional Conduct and Ethics for Registered Medical Practitioners (Amended)' (2016) last updated 2019 (Ireland). www.medicalcouncil.ie/news-and-publications/reports/guide-to-professional-conduct-ethics-8th-edition.html accessed 26 March 2024).

(Model-)Professional Code for Physicians in Germany *((Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte MBO-Ä 1997*) (Germany). www.aerzteblatt.de/archiv/198641/(Muster-)Berufsordnung-fuer-die-in-Deutschland-taetigen-Aerztinnenund-Aerzte-in-der-Fassung-der-Beschluesse-des-121-Deutschen-Aerztetages-2018-in-Erfurt

Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslag (2009:400)*) (Sweden).

Policy documents

Article 29 Data Protection Working Party (WP29),—— 'Working Document on the processing of personal data relation to health in electronic health records (EHR)' (2007) 15 February 2007, WP 131.

Article 29 Data Protection Working Party (WP29), 'Opinion 05/2014 on Anonymisation Techniques' (2014) 10 April 2014, WP216.

Council of Europe,—— 'Protection of health-related data' Recommendation CM/Rec(2019)2 (2019). https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html

Council of Europe, Oviedo Convention, Explanatory report. https://www.coe.int/en/web/bioethics/oviedo-convention

Council of the European Union, 'Proposal for a Regulation on the European Health Data Space Analysis of the final compromise text with a view to agreement' (2022) 2022/0140(COD) (EHDS (compromise text).

EDPB-EDPS, 'Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' (2022) 12 July 2022.

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 European strategy for data' (2020) COM/2020/66 final.

European Data Protection Board (EDPB), 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0' (2019) 20 October 2020.

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

European Parliament, 'Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' (2023) (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))(1), T9-0462/2023. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0140(COD)&l=en

MedTech Europe, 'Unlocking the full benefits of health data. Recommendations from MedTech Europe' (2021) position paper, 16 June 2021. https://www.medtecheurope.org/wp-content/uploads/2021/06/mte_160621_positionpaper_health-data.pdf

The European Data Protection Supervisor (EDPS), 'A preliminary opinion on data protection and scientific research' (2020) 6 January 2020.
World Medical Association (WMA), Declaration of Geneva, 1948. https://www.wma.net/policies-post/wma-declaration-of-geneva/
World Medical Association (WMA),—— Declaration of Geneva, the 'Modern Hippocratic Oath'. (n.d.). https://www.wma.net/what-we-do/medical-ethics/declaration-of-geneva/
World Medical Association (WMA),—— Declaration of Lisbon on the rights of the patient. https://www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/
World Medical Association (WMA),—— WMA International Code of Medical Ethics. https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/

Literature and other secondary sources

Abbing HR, 'Medical confidentiality and patient safety: Reporting procedures' (2014) 21(3) *European Journal of Health Law* 245–259. https://doi.org/10.1163/15718093-12341319
Cimina V, 'The proposal for a European Health Data Space: Between pursued objectives and data protection challenges' (2023) 24 *ERA-Forum* 343–359. https://doi.org/10.1007/s12027-023-00764-7
Data Saves Lives, 'Why is health data important?' (n.d.). www.datasaveslives.eu/why-is-health-data-important
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), 'Register im Gesundheitsbereich'. (n.d.). www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/Allgemein/RegisterimGesundheitsbereich.html
Dove ES, 'Confidentiality, public interest, and the human right to science: when can confidential information be used for the benefit of the wider community?' (2023) 10(1) *Journal of Law and the Biosciences* lsad013. https://doi.org/10.1093/jlb/lsad013
European Parliament, 'EP supports creating EU Health Data Space to boost access to data and research' (2023) press release, 13 December 2023. www.europarl.europa.eu/news/en/press-room/20231208IPR15783/ep-supports-creating-eu-health-data-space-to-boost-access-to-data-and-research
Fåhraeus D, Reichel J and Slokenberga S, 'The European Health Data Space: Challenges and Opportunities' (2024) European Policy Analysis, Sieps – Swedish Institute for European Policy Studies, February 2024. www.sieps.se/en/publications/2024/the-european-health-data-space/
Hartlev M, 'Forwards or backwards? New directions in Danish patients' rights legislation' (2011) *European Journal of Health Law* 18(4), 365–374. https://doi.org/10.1163/157180911X575758
Katzenmeier C, 'Berufsgeheimnis und Dokumentation' in Laufs A, Katzenmeier C and Lipp V, Arztrecht. Verlag C.H. Beck oHG (2021).
Ludmila G and Kuner C, 'Article 9 Processing of special categories of personal data', in Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) online edn, Oxford Academic, 365–384. https://doi.org/10.1093/oso/9780198826491.003.0038
Raab R and others, 'Federated electronic health records for the European Health Data Space' (2023) 5 *Lancet Digit Health* e840–e847. https://doi.org/10.1016/S2589-7500(23)00156-5
Rumbold JMM and Pierscionek B, 'The effect of the general data protection regulation on medical research' (2017) 19(2) *Journal of Medical Internet Research* e47. https://doi.org/10.2196/jmir.7108
Schmidt H and Callier S, 'How anonymous is "anonymous"? Some suggestions towards a coherent universal coding system for genetic samples' (2012) 38(5) *Journal of Medical Ethics* 304–309. https://doi.org/10.1136/medethics-2011-100181

Slokenberga S, 'Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along' (2022) *Technology and Regulation* 135–147. https://doi.org/10.26116/techreg.2022.014

Sokalska, M, 'Medical confidentiality – Quo Vadis?' (2004) 11(1) *European Journal of Health Law* 35–43. https://doi.org/10.1163/1571809043230423 26

Spajic D, 'Patient data sharing for the improvement of healthcare and medical research: Towards a moral duty of patients to share health-related data?' (2023) (PhD Dissertation, KU Leuven 2023).

Standing Committee of European Doctors (CPME), 'European doctors call for more ambition on professional secrecy and patient confidentiality in European Health Data Space', 8 February 2024. https://www.cpme.eu/news/european-doctors-call-for-more-ambition-on-professional-secrecy-and-patient-confidentiality-in-european-health-data-space

Time.lex, Milieu, 'Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations' (2014) 23 July 2024. https://health.ec.europa.eu/other-pages/basic-page/overview-national-laws-electronic-health-records-eu-member-states-2016_en

Vedder A and Spajic D, 'Moral autonomy of patients and legal barriers to a possible duty of health related data sharing' (2023) 25 *Ethics and Information Technology* 23. https://doi.org/10.1007/s10676-023-09697-8

Case law

Armonas v Lithuania App no. 36919/02 (ECtHR, 25 November 2008).

Biriuk v Lithuania App no 23373/03 (ECtHR, 25 November 2008).

Biržietis v Lithuania App no. 49304/09 (ECtHR, 14 June 2016).

Handyside v the United Kingdom App no. 5493/72 (ECtHR, 07 December 1976).

Kiyutin v Russia no. 2700/10 (ECtHR, 10 March 2011).

LH v Latvia App no 52019/07 (ECtHR, 29 April 2014).

Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).

Panteleyenko v Ukraine App no 11901/02 (ECtHR, 29 June 2006).

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000).

S and Marper v the United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008).

Z v Finland App no 22009/93 (ECtHR, 25 February 1997).