EHDS AS A STEPPING STONE TO SECONDARY USES OF PERSONAL HEALTH DATA FOR SCIENCE AND RESEARCH

Lucie Široká[1]

Abstract: The paper analyses the legal framework for the processing of personal data in healthcare within the European Union, focusing on the secondary use of health data for scientific and research purposes. The first part defines the roles of controllers and processors, the categories of processed data, and the legal grounds for primary processing under the GDPR. It highlights that medical records are an indispensable tool for ensuring continuity of care and constitute evidence of *lege artis* practice. The text then distinguishes between anonymisation and pseudonymisation, explaining their importance and limitations for research: anonymisation places data outside the scope of the GDPR, yet in many domains it remains practically or methodologically unattainable; pseudonymisation, by contrast, falls within the regulatory scope and functions as a safeguard of security, rather than as a pathway to "non-personal" data. Furthermore, the paper discusses the weaknesses of relying on research consents (asymmetry, logistical burdens, revocability) and the limited applicability of the compatibility of purposes doctrine in the absence of specific legislation. The core of the paper is the introduction of the European Health Data Space (EHDS) Regulation, which imposes an obligation upon data holders to make defined categories of electronic health data available for specified secondary purposes, defines data users, prohibits discriminatory and marketing use, and establishes Health Data Access Bodies as independent intermediaries with supervisory functions. The paper evaluates EHDS as a significant step towards an institutionally and technically robust model of secondary data use that can reconcile privacy protection with the legitimate goals of science.

Resumé: Text analyzuje právní rámec zpracování osobních údajů ve zdravotnictví v Evropské unii se zaměřením na sekundární využití zdravotních dat pro účely vědy a výzkumu. V první části vymezuje role správců a zpracovatelů, kategorie zpracovávaných údajů a právní tituly primárního zpracování dle GDPR. Ukazuje, že zdravotnická dokumentace je nezbytným nástrojem kontinuity péče a důkazem *lege artis* postupu. Následně rozlišuje anonymizaci a pseudonymizaci a vysvětluje jejich význam a limity pro výzkum: anonymizace vyvádí data z působnosti GDPR, avšak je v řadě domén prakticky či metodologicky nedosažitelná; pseudonymizace naopak zůstává uvnitř regulace a slouží jako záruka bezpečnosti, nikoli jako cesta k „ne-osobním" údajům. Text se věnuje slabinám opory ve výzkumných souhlasech (asymetrie, logistika, odvolatelnost) a omezené použitelnosti doktríny slučitelnosti účelů bez specifické legislativy. Těžištěm práce je představení nařízení EHDS, které zavádí povinnost držitelů dat zpřístupňovat definované kategorie elektronických zdravotních údajů pro vymezené sekundární účely, vymezuje uživatele dat, zakazuje diskriminační a marketingové použití, a zřizuje Health Data Access Bodies jako nezávislé zprostředkovatele s dohledovou funkcí. Předložený text hodnotí EHDS jako významný krok k institucionálně a technicky robustnímu modelu sekundárního využití dat, který může sladit ochranu soukromí s legitimními cíli vědeckého bádání.

[1] *This article was written with support of the Specific University Research (SVV) project of Charles University No. 260748 "Challenges of Private Law: sustainability and technology".*

Key words: Data protection; EHDS; GDPR; secondary use of health data; further processing of health data

On the author:

JUDr. Lucie Široká, Ph.D., is a lecturer at the Department of Medical Law and the Department of Civil Law, Charles University Faculty of Law. Her areas of expertise include data protection in healthcare, digitisation of healthcare, and cybersecurity.

Introduction

The provision of healthcare services represents an area of human activity that is inherently connected with the processing of personal data. Without the proper collection of patient history, the establishment of diagnoses, the indication and prescription of appropriate interventions, and their systematic documentation, healthcare could not be delivered at the required professional level (so-called *lege artis*). The collection, storage, classification, evaluation, and retention of patient data are prerequisites for the proper provision of healthcare. Delivering healthcare services in compliance with *lege artis* standards constitutes an obligation incumbent upon providers[2]. At the level of international public law, this duty is enshrined in the Convention on Human Rights and Biomedicine (Council of Europe, 1997)[3][4].

In the Czech Republic, the obligation of providers to deliver healthcare at the appropriate professional standard is reflected in sector-specific legislation — e.g. § 45(1) of the Health Services Act[5] — as well as in the private law codex, the Civil Code, which requires providers to act with the care of a duly qualified professional (§ 2643(1) Civil Code)[6]. Comparable provisions exist in other continental European systems, including Germany[7] and France[8].

Since 25 May 2018, the Member States of the European Union have been bound by a generally applicable legal act defining the rights and obligations related to the processing of personal data of natural persons — 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"). The GDPR applies across a wide range of human activities, including healthcare, and together with specific legislation

[2] For an overview of the influence of modern digital technologies, particularly medical AI systems, on the standard of care (lex artis), see ŠUSTEK, Petr. AI in Medicine and the Standard of Care, in this volume of the *Czech Yearbook of International Public & Private Law*. For considerations regarding the importance of personal data protection for the physician–patient relationship, see ŠOLC, Martin. Is There a Right for the Human Touch? AI and the Future of the Physician-Patient Relationship, in this volume of the *Czech Yearbook of International Public & Private Law*.

[3] Council Of Europe. Convention on Human Rights and Biomedicine. Oviedo, 4 April 1997.

[4] Constitutional Court of the Czech Republic. Decision Pl. ÚS 36/01 of 25 June 2002.

[5] Act No. 372/2011 Coll., on Health Services and Conditions of Their Provision [Zákon o zdravotních službách a podmínkách jejich poskytování]

[6] Act No. 89/2012 Coll., the Civil Code [Občanský zákoník]. For more details, see e. g. ŠUSTEK, P. Professional Standards. In: HOLČAPEK, T., ŠUSTEK, P., ŠOLC, M. *Czech Health Law*. Praha: Wolters Kluwer ČR, 2023. pp. 33–40.

[7] Bürgerliches Gesetzbuch (BGB). § 630a(2).

[8] Code De La Santé Publique (FR). Article L1110-5-1.

governing the provision of health services establishes the legal basis and framework for lawful processing of personal data in patient care.[9]

Healthcare systems generate vast amounts of personal data of immense informational value, with considerable potential, particularly in the context of science and research. Yet, the secondary use and processing of health data is legally complex. Reinforcement of the position of research institutions in this field is provided by the adoption of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.

The aim of this text is to demonstrate the complexities of secondary processing of personal data for research purposes under the existing EU legal framework (*de lege lata*) and to introduce the changes brought about by the EHDS in this area.

1. Processing of Personal Data in Healthcare

For the lawful processing of personal data, it is essential that the roles of the entities involved are properly allocated and that the full life cycle of the personal data in question is appropriately mapped[10].

1.1 The Position of Data Subjects and Allocation of Roles

The patient is the recipient of healthcare. At the same time, the patient is a contractual party to the healthcare contract, which creates a legal relationship between the patient and the provider, or, where applicable, a beneficiary under a contract for the benefit of a third party. From the perspective of the GDPR, the patient qualifies as a data subject, i.e. a natural person who is identified or can be identified, directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, network identifier, or to one or more specific factors relating to the physical, physiological, genetic, psychological, economic, cultural, or social identity of that natural person[11].

With regard to the allocation of roles, it is clear that, in their relation to patients as data subjects (Article 4(1) GDPR), healthcare providers act as controllers of personal data, since they determine the purpose and means of processing. Patients' personal data are primarily processed in order to maintain medical documentation, which functions as a source of information for treating practitioners, as a prerequisite for the continuity of care, as a tool to prevent duplicative or disproportionately burdensome examinations, and as proof of the care provided.[12]

Where a provider uses information systems or software solutions for the processing of personal data, such systems are typically supplied by a specialised vendor within contractual supply relationships. Processing does not necessarily need to be carried out by the controller

[9] There are, of course, several approaches to addressing privacy protection. See e. g. BENNETT, C.J., & Raab, C.D. (2003). *The Governance of Privacy: Policy Instruments in Global Perspective* (1st ed.). Routledge. https://doi.org/10.4324/9781315199269.

[10] European Data Protection Board. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Version 2.1, 07.10.2020. Available at: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[11] GDPR, Article 4(1).

[12] See also HOLČAPEK, T. Medical Records. In: HOLČAPEK, T., ŠUSTEK, P., ŠOLC, M. *Czech Health Law*. Praha: Wolters Kluwer ČR, 2023. pp. 59–61.

itself. Specific processing operations or broader arrangements involving the processing of personal data may be outsourced to processors[13]. A supplier that processes personal data on behalf of the healthcare provider thus acts as a processor, as it processes data on the controller's instructions and under its responsibility[14].[15]

1.2 Categories of Personal Data Processed in Healthcare, Legal Grounds and Purpose of Processing

In the course of providing healthcare services, both "standard" personal data in the sense of Article 4(1) GDPR — such as identification or address data — and special categories of personal data within the meaning of Article 9(1) GDPR are processed. The latter include sensitive information such as data concerning health status, genetic data (DNA, RNA, Rh factor), and, where relevant, biometric data.

To comply with the principle of lawfulness of processing[16] and the principle of purpose limitation[17], it is necessary to clearly isolate the specific purpose of the processing and the corresponding legal ground.

Healthcare providers process personal data for the primary purpose of delivering healthcare to the individual patient. The relevant lawful basis may be found in Article 6(1)(b) GDPR (processing necessary for the performance of a contract to which the data subject is party) or Article 6(1)(c) GDPR (processing necessary for compliance with a legal obligation to which the controller is subject). In the European context, contracts are generally concluded for the provision of non-acute, planned care, obliging the healthcare provider to treat the patient with the care of a duly qualified professional. In cases where urgent, life-saving care is required, and the patient is not able to enter into a contractual relationship, another legal basis must be identified. In such cases, processing is covered under Article 6(1)(c) GDPR, as processing necessary to comply with a legal obligation imposed on the provider; if no such obligation were defined in national law, Article 6(1)(d) GDPR (processing necessary in order to protect the vital interests of the data subject or another natural person) may be applicable.

These legal grounds suffice for the lawfulness of processing "standard" personal data. For the lawful processing of special categories of personal data, however, an additional derogation under Article 9(2) GDPR must also apply[18]. Pursuant to Article 9(1) GDPR, the processing of data concerning health, genetic data, biometric data for unique identification purposes, or similar sensitive data is in principle prohibited. To allow such processing, a specific exception must be satisfied. For the purposes of providing healthcare, the applicable derogation is Article 9(2)(h) GDPR, which permits processing necessary for purposes such as preventive or occupational medicine, assessment of an employee's working capacity, medical diagnosis,

---

13 ŠIROKÁ, L. In: HOLČAPEK, T., ŠUSTEK, P., ŠOLC, M. and ŠIROKÁ, L. *Právní nástroje podpory inovací v medicíně*. [Legal instruments to support innovation in medicine] Praha: Wolters Kluwer ČR, 2024. p. 61.

14 GDPR, Article 4(8).

15 For further details, please refer to *EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR* and/or KUNER, Ch. and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Law Pro), https://doi.org/10.1093/oso/9780198826491.001.0001, accessed 18 Sept. 2025.

16 GDPR, Article 5(1)(a).

17 GDPR, Article 5(1)(b).

18 ŠIROKÁ, L. In: ŠUSTEK, P., HOLČAPEK, T., ŠIROKÁ, L., ŠOLC, M. *Zákon o zdravotních službách. Komentář*. [Health Services Act. Commentary.] Praha: Wolters Kluwer ČR, 2024. p. 321.

provision of health or social care or treatment, or the management of health or social care systems and services, provided such processing is carried out under Union or Member State law, or pursuant to a contract with a healthcare professional.

It is therefore clear that the processing of both categories of personal data for the purpose of providing healthcare to a particular patient generally takes place without the patient's consent[19, 20].

Healthcare providers undeniably hold extensive databases of personal data. These data are extremely valuable and of fundamental significance for potential research. Their secondary use, if permitted, may contribute not only to medical progress but also to the benefit of society at large.

2. Possibilities of Secondary Processing of Personal Data Collected in Healthcare for Research Purposes under the Legal Framework *de lege lata*

The regulatory sources governing secondary processing of personal data are found primarily in the GDPR and in national legislation of the EU Member States. It has become evident that, contrary to initial expectations, the GDPR alone is not sufficient for this purpose. The actual execution of secondary use of health data requires a strong, domestic legal regulation.

2.1 Anonymisation and Pseudonymisation

When considering the secondary use of health data collected by healthcare providers, it is necessary to reflect on the nature of anonymised and pseudonymised data. Both are expressions frequently used in the context of research.[21] When personal data are anonymised, they become anonymous data. Anonymous data are those through which an individual can no longer be identified, either directly or indirectly, even with the aid of additional instruments, lists, or resources. Such data fall outside the scope of the GDPR. Recital 26 GDPR explicitly states that "*the principles of data protection should not apply to anonymous information*", namely information which does not relate to an identified or identifiable natural person, as well as to personal data rendered anonymous in such a way that the data subject is not, or no longer is, identifiable. Consequently, GDPR does not apply to the processing of such anonymous information, including its use for statistical or research purposes. Handling of such information will instead be influenced by general principles like good morals.

It must nevertheless be emphasised that anonymisation itself represents a processing operation, carried out with personal data at the outset, and therefore it must comply with GDPR requirements for lawful and purpose-limited processing.

---

[19] Office For Personal Data Protection (CZ). *Opinion No. 3/2014 on Excessive Requirement for Consent to the Processing of Personal Data and Related Incorrect Fulfilment of the Information Duty*. Prague: ÚOOÚ, 2014.

[20] Of course, if a healthcare provider processes patients' personal data for other purposes, such as promoting and presenting certain services, the healthcare provider needs to find another suitable legal basis for processing personal data.

[21] For a more detailed discussion of the difference, see *EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act).*

From the perspective of research demands, anonymisation may appear as a desirable pathway in support of science and research, not least in light of prevailing ethical considerations. For example, the Czech Republic amended the Health Services Act to expressly allow further use of patient medical records for research purposes, provided the data are anonymised to the extent that the patient's identity cannot be established. In such a case the resulting information no longer qualifies as medical documentation[22]. Here, the legal basis for anonymisation is directly provided by a special legal act, and anonymisation is entrusted to healthcare providers in their role as controllers. This creates practical feasibility but also presupposes the active involvement of providers themselves: researchers have no legal right to access medical documentation directly and cannot themselves select the necessary data.

While this kind of legislative facilitation appears favourable at first glance, it would be an overstatement to see it as a comprehensive solution for research data access. Anonymisation, although conceptually laudable, is in the healthcare context often logically or technically impossible. Anonymous data are only those for which an individual can no longer be identified. Thus, anonymisation is not merely the removal of some identifiers, if re-identification by reasonable means remains possible[23]. It is therefore erroneous to assume, as is sometimes the case in practice, that deleting a patient's name, birth date, or address suffices to render the data anonymous.

In many institutions, an alternative approach is used: each patient is assigned a unique code or identifier separate from identifying information, while unnecessary personal data are removed. The link key is stored separately. However, this process does not yield anonymous data. Rather, it results in pseudonymised data. Pursuant to Article 4(5) GDPR, pseudonymised data are still personal data and thus remain subject to the GDPR[24]. Pseudonymisation undoubtedly strengthens the protection of personal data, supporting integrity, availability, and confidentiality, yet it does not transform personal data into non-personal data.[25]

For research purposes, pseudonymisation is frequently indispensable: fully anonymised data may lack scientific utility and may not be sufficient to answer the intended research questions. Many forms of data, particularly imaging results or genomic sequences, cannot be meaningfully anonymised without stripping away their essential value. In these cases, researchers require access to the primary data.

2.2 Activation of Controllers

Another complex issue concerns the role of research organisations that are not providers of healthcare. If anonymisation is legally entrusted to providers, are they obligated to perform anonymisation upon request by researchers? Healthcare providers hold datasets of immense scientific potential but may lack any interest in conducting the research themselves. Researchers, however, cannot directly access medical documentation. Their access is contingent upon the cooperation and active engagement of providers. At present, no independently applicable legal basis grants researchers the right to such access for secondary use.

---

22 Act No. 372/2011 Coll., Section 55b, on Health Services.

23 Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. WP216. 10 April 2014.

24 GDPR, Article 4(5).

25 For a more detailed discussion of the limits of anonymization, see OHM, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, Vol. 57, 2010.

2.3 Searching for a Legal Path

It may be considered whether the legal ground for the processing of personal data under Article 6(1)(e) GDPR could apply, which provides that processing shall be lawful where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. However, identifying a public interest is particularly difficult in the case of commercial clinical trials. In addition, it is necessary to rely on an exception for the processing of special categories of personal data. The only potentially relevant exception appears to be that laid down in Article 9(2)(j) GDPR: *processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), based on Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific safeguards to protect the fundamental rights and interests of the data subject*. All of this is supported by Article 89 GDPR, which establishes the requirement of safeguards, but at the same time allows for possible derogations relating to processing for archiving in the public interest, scientific or historical research purposes, or statistical purposes. As regards both safeguards and possible derogations, there is an urgent lack of further guidance or national legislation.

Even if, despite these difficulties, we were to conclude that processing for research purposes is lawful, researchers still lack a means to access the data contained in patients' medical records. The legal orders of individual EU Member States set rules for access to data contained in medical documentation and simultaneously impose a strict duty of confidentiality, which can be lifted only under conditions laid down by public law provisions. Consequently, with regard to data contained in medical records, scientists and researchers are reliant on the patient's consent.

In view of the uncertainties surrounding the application of these provisions, the prevailing practice is to obtain the consent of the data subjects concerned—both for access to the data and for their processing for the purpose of conducting the scientific research project.

2.4 Patient Consent

Because of these obstacles, patient consent has become the principal instrument applied in practice. Yet reliance on consent is fraught with problems. The patient represents the weaker party in the relationship with providers or research institutions. Patients may be dependent on healthcare providers and may not be in a position to exercise free choice.

In retrospective studies, it is practically impossible to retrieve valid consents from large numbers of past patients. Prospective studies encounter additional complications: why should a patient agree to participate in research involving their personal data? Often the motivation lies in a hope for treatment, relief, or other personal benefit, which calls into question whether consent is truly given freely. Moreover, under Article 7 GDPR, consent is revocable at any time and for any reason[2627]. Such instability[28] undermines legal certainty, while the process of organising large-scale consent collection places heavy logistical burdens

[26] Court of Justice of the European Union. Judgment of 19 October 2016, Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland.

[27] GDPR, Article 7.

[28] European Data Protection Board. *Guidelines 03/2020 on processing of health data for research purposes in the context of COVID-19*. 2020.

on institutions. Methodologically, it may also skew data sets, as patients agreeing to provide consent may not be representative.

Thus, although consent is widespread as a basis for research processing, it is legally fragile, unstable, and operationally problematic.

2.5 Compatibility of Purposes

Another possible approach is reliance on the principle of compatibility of purposes. GDPR Recital 50 explicitly mentions processing for scientific research as purposes that may be considered compatible with the initial purposes of data collection[29]. Article 5(1)(b) GDPR allows such compatibility. Nevertheless, Article 6(4) GDPR sets out strict legal-technical conditions for its application. Where primary processing already takes place without patient consent — as is the case in the provision of healthcare — and no specific legislative basis for secondary research use exists, compatibility cannot readily be invoked[30].

2.6 Interim Summary

The position of research organisations seeking to work with patient data under the current legal regime is therefore highly problematic. European healthcare systems face a profound paradox. On the one hand, vast amounts of data are collected daily. On the other, much of this information remains locked away in isolated systems, inaccessible to purposes other than direct patient care.

---

[29] GDPR, Recital 50: *The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their 4.5.2016 EN Official Journal of the European Union L 119/9 further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.*

[30] GDPR, Article 6(4): *Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.*

The reasons are complex, but at their core lie legal and institutional barriers. The GDPR, while providing a high level of protection, was never primarily designed to facilitate extensive, cross-border secondary uses of health data.

The challenges of secondary use sit at the intersection of fundamental rights. On one side stands the right to privacy and data protection (Article 8 Charter of fundamental rights of the European union[31], Article 16 Treaty on the Functioning of the European Union[32]), grounded in the principle of informational self-determination. On the other side are pressing public interest[33] objectives: the right to health protection (Article 35 Charter of fundamental rights of the European union), support of scientific research (Article 179 Treaty on the Functioning of the European Union), and the goal of achieving a high level of human health protection[34].

The reliance upon individual consent, while offering certainty from a formal point of view, does not provide the necessary stability or flexibility. Securing specific, informed, and freely given consent from millions of patients for thousands of potential projects is not feasible. It entails an enormous logistical effort and risks distorting datasets.

Beyond this, it must be recalled that the GDPR applies only to data relating to living individuals. Yet medical records are archived for periods surpassing human life spans. Consequently, some parts of patient records — namely data relating to deceased persons — may fall outside GDPR protection and thus might be usable under less restrictive conditions.

Academic and policy debates therefore increasingly call for a new model — one capable of moving beyond individualist control of personal data and towards a system reflecting their collective societal value. Such a model must rest on principles of trust, transparency, accountability, and robust legal-technical safeguards. EHDS represents an attempt to codify precisely such an approach.

3. Secondary Processing of Health Data for Research Purposes from the Perspective of EHDS

The EHDS introduces a dedicated regulation of secondary use of personal health data, contained in Articles 50 et seq. Its purpose is to approach secondary use with maximum openness, promoting the widest possible exploitation of existing datasets across the Union. Enormous amounts of health data have been accumulated throughout the EU. These data offer the potential to advance scientific knowledge both by building on existing information and by enabling novel forms of analysis.

The objective of EHDS is *to establish a common mechanism for access to electronic health data for secondary purposes throughout the Union. Within this mechanism, health data holders are*

[31] Charter of fundamental rights of the European union. OJ C 202, 7.6.2016, pp. 389–405.

[32] Consolidated Version of the Treaty on n the Functioning of the European Union. OJ C 202, 7.6.2016.

[33] For more details see PURTOVA, N. *Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons* in LEENES, R., PURTOVA, N., ADAMS, S. (eds.) (2017) Under Observation – The Interplay Between eHealth and Surveillance. Springer, *Tilburg Law School Research Paper No. 15/2016.*

[34] A high level of human health protection is one of the objectives of the European Union, as laid down in the Treaty on the Functioning of the European Union (Article 168 Treaty on the Functioning of the European Union). Specifically, Article 168 provides that a high level of human health protection shall be ensured in the definition and implementation of all Union policies and activities. This objective is also reflected in other EU legislation and policies.

obliged to make the data in their possession available subject to permits and approved requests[35]. To this end, EHDS defines relevant concepts, establishes legal grounds for secondary use of personal data, and specifies detailed procedural steps.

EHDS is built on two interrelated pillars. The first pillar concerns primary use of data (MyHealth@EU), reinforcing EU citizens' rights of access and control over their health data and facilitating cross-border healthcare.[36] It aims to ensure that core documents such as patient summaries or electronic prescriptions are accessible and usable in every Member State. This depends upon mandatory certification of electronic health record systems (EHR) and the creation of a European format for EHR.

The second pillar concerns secondary use of data (HealthData@EU). This establishes the legal and technical framework for using health data for research, innovation, and other defined secondary purposes. Though distinct, the two pillars are interlinked: high-quality, interoperable data in primary care represent a prerequisite for high-quality datasets suitable for research.

3.1 Data Holders

EHDS creates a new legal category of data holders, meaning any public or private entity (typically healthcare providers or public authorities administering registries) that collects and processes defined categories of electronic health data (Article 2(2)(t) EHDS)[37].

The key innovation is that these data holders are subject to a legal obligation to make their data available for secondary use once a request is approved by the competent authority. Article 51(1) EHDS lists the categories of data to be provided[38]. As a result, data holders

---

35 EHDS, Recital 52.

36 EHDS through the perspective of European Data Protection Board and European Data Protection Supervisor see *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*.

37 The data holder is defined like „*any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, 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 the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency, that has either: (i) the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policymaking, official statistics or patient safety or for regulatory purposes; or (ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data.*"

38 (a) electronic health data from EHRs; (b) data on factors impacting on health, including socioeconomic, environmental and behavioural determinants of health; (c) aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing; (d) data on pathogens that impact human health; (e) healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements; (f) human genetic, epigenomic and genomic data; (g) other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other omic data; (h) personal electronic health data automatically generated through medical devices; (i) data from wellness applications; (j) data on professional status, and on the specialisation and institution of health professionals involved in the treatment of a natural person; (k) data from population-based health data registries such as public health registries; (l) data from medical registries and mortality registries; (m) data from clinical trials, clinical studies, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council (35), Regulation (EU) 2017/745 and Regulation (EU) 2017/746; (n) other health data from medical devices; (o) data from registries for medicinal products and medical devices; (p) data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results; (q) health data from biobanks and associated databases.

are transformed from passive custodians into active actors within the data ecosystem, with a clearly defined duty to contribute to secondary processing.

Among the permitted purposes for access is scientific research related to health or care sectors that contributes to public health or health technology assessment, or ensures high levels of quality and safety of care, medicinal products, or medical devices. This includes, inter alia, (i) development and innovation of products and services, and (ii) training, testing, and evaluation of algorithms, including in medical devices, in vitro diagnostic technologies, AI systems, and digital health applications (Article 53(1)(e) EHDS).

3.2 Data Users

On the other side are the data users, which may include public institutions, universities, research organisations, and private companies. Health data users shall only process electronic health data for secondary use on the basis of and in accordance with the purposes contained in a data permit issued pursuant to Article 68 EHDS, health data requests approved pursuant to Article 69EHDS or, in situations referred to in Article 67(3) EHDS, an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75 EHDS.

In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 EHDS or a health data request approved pursuant to Article 69 EHDS for the following uses shall be prohibited:

a) taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; in order to qualify as 'decisions' for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;
b) taking decisions in relation to a natural person or a group of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained;
c) carrying out advertising or marketing activities;
d) developing products or services that may harm individuals, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction, contravene public order or cause a risk for human health;
e) carrying out activities in conflict with ethical provisions laid down in national law.[39]

3.3 Health Data Access Bodies

A novel institutional feature of EHDS is the creation of Health Data Access Bodies (HDABs) in each Member State. These must be functionally independent and act as trusted intermediaries. Their tasks include: receiving and reviewing applications from data users; issuing access permits; ensuring compliance with the principle of data minimisation; operating or supervising secure data processing environments; ensuring public transparency

[39] EHDS, Article 54.

by publishing details of issued permits; and cooperating within the HealthData@EU network[40].

HDABs are empowered to supervise data users' compliance with permit conditions and may impose sanctions where necessary. In cases of violation — e.g. attempts at re-identification or use of data for unauthorised purposes — an HDAB may revoke the permit and initiate proceedings under the GDPR, including significant fines.

3.4 Access to Health Data

The process of obtaining access begins with an application submitted by a natural or legal person. Article 67(2) EHDS sets out the required content of applications. For cross-border projects, a single application must still be submitted to only one HDAB. This HDAB assesses the request against formal and substantive criteria: whether the purpose aligns with permitted secondary uses; whether the scope requested complies with the principle of necessity and proportionality (data minimisation); and whether the applicant can demonstrate adequate technical and organisational safeguards[41].

If approved, the HDAB issues a legally binding permit specifying the datasets, duration, and exact conditions of processing[42].

Where the applicant seeks access only to anonymised statistical outputs, Article 69 EHDS permits this. In such cases, the HDAB may only provide results in anonymised statistical formats. Under no circumstances may data users directly obtain or download identifiable electronic health data.

3.5 Legal Bases for Processing under EHDS

A crucial contribution of EHDS is the elimination of legal uncertainty through the explicit codification of lawful grounds for secondary processing.

For data holders, the obligation to provide data constitutes a legal obligation under Article 6(1)(c) GDPR, in combination with the derogations of Article 9(2)(i) and (j) GDPR.

Health Data Access Bodies act under Article 6(1)(e) GDPR (task carried out in the public interest) combined with Article 9(2)(g)–(j) GDPR.

Data users may rely on Article 6(1)(a), (c), (e), or (f) GDPR in conjunction with Article 9(2)(g)–(j), with EHDS defining the necessary safeguards[43].

A major innovation is the introduction of the individual right to refuse secondary use of one's personal electronic health data under EHDS. This right may be exercised at any time and without justification. Member States must establish procedures for such opt-outs, though they may also provide for domestic rules allowing access to data even when an opt-out has been lodged, depending on the balance with overriding public interests.

40 EHDS, Articles 55–59.
41 EHDS, Article 68(1).
42 EHDS, Article 68(10).
43 EHDS, Recital 52.

Conclusion

The present text demonstrates that the provision of healthcare is inherently a data-intensive activity in which the legitimate demands of patient privacy and informational self-determination intersect with pressing public interests in promoting research and enhancing the quality of care. Primary processing of personal data for *lege artis* healthcare delivery rests on clearly delineated roles of the entities involved, grounded principles of GDPR (lawfulness, purpose limitation, data minimisation, integrity and confidentiality), and on adequate lawful bases under Article 6 combined with exceptions under Article 9(2) GDPR. Medical documentation thus functions both as a tool for correct professional treatment, the preservation of continuity of care, prevention of duplication or excessive burdens on patients, and as legal proof of due practice.

Secondary use of health data — whether for retrospective studies, registries, or the development and validation of algorithms — encounters, under the current *de lege lata* framework, significant legal and practical limitations. The distinction between anonymisation and pseudonymisation is of central importance. Anonymisation, understood as irreversible de-identification under the "reasonably likely means" test, removes data from the scope of GDPR yet proves, in many clinical areas, either unfeasible in practice without destroying the scientific value (e.g. genetics, imaging) or methodologically inadequate. Pseudonymisation, conversely, remains within the scope of regulation, providing important safeguards, but does not convert personal data to "non-personal" status. Reliance upon patient consent as a universal solution is legally precarious and empirically unstable in the healthcare context.

In this setting, the EHDS represents a fundamental institutional innovation. It creates the role of data holders with a duty to provide defined categories of electronic health data for legitimate secondary purposes; it delineates the position of data users, sets binding prohibitions, and establishes Health Data Access Bodies as neutral overseers with supervisory competence. This dual innovation both reduces uncertainty surrounding lawful bases for processing (for data holders, data users, and access bodies) and creates procedural standards for safe use of health data within secure environments and under minimisation principles.

The EHDS does not eliminate all challenges. It is designed primarily for electronic data, whereas historical paper datasets and uneven digitalisation across Member States may hinder its effective implementation in transitional periods. The establishment of a European Health Data Space introduces considerable cybersecurity challenges. Moreover, vast amounts of data not covered by GDPR (for example, data on deceased patients) remain in data holders' repositories; for these, methodological guidance enabling their secondary use would be highly appropriate.

Nevertheless, EHDS provides a vital step forward, offering the kind of legal certainty urgently needed to support scientific research. It lays the foundations for an institutionally and technically robust model of secondary data use — one capable of reconciling personal data protection with the legitimate objectives of science, innovation, and public health.