OPEN FOR FEEDBACK

From concerns to consent: addressing the issue of trust and other challenges impairing secondary use of health data in Poland and beyond

ODI Fellowships: report

January 2024

Open Data Institute

Contents

About

This report was produced as part of the ODI research fellow scheme. Its author was Blanka Wawrzyniak, Head of the Digital Economy Programme at Instrat Foundation, with contributions from Lucas Stliglich and Joe Massey, ODI.

If you want to share feedback by email or would like to get in touch, contact Blanka at blankawawrzyniak@gmail.com.

If you would like to learn more about the ODI research fellow scheme, please visit the information and application page or contact us at fellowships@theodi.org.

ODI Fellowships

This report is authored by an ODI fellow. It draws on concepts developed by the ODI but the author's views are their own.

Executive summary

The report explores the secondary use of health data and citizen engagement in the health data-sharing process. The study refers to the development of the European Health Data Space (EHDS), while focusing primarily on the Polish context. In analysing the major obstacle impeding the sharing of health data for secondary use – namely, the lack of trust – the report investigates why this barrier is particularly prominent in Poland and endeavours to find solutions to mitigate it. The analysis also refers to other aspects influencing health data reuse, such as regulatory barriers, lack of proper infrastructure and technical standards, and lack of awareness of patients and medical staff. Subsequently, the report puts forth several recommendations aimed at establishing the foundation for the evolution of the digital health data space. In addition to addressing elements commonly discussed in healthcare digitisation discourse, such as legal clarity and data interoperability, the report places substantial emphasis on societal aspects. It underscores the significance of cultivating trust and motivating citizens to actively contribute to the success of the forthcoming digital health data space.

Key recommendations:

- Building trust through design and democratic governance of the data-sharing models (societal aspect),
- Raising citizens' awareness (societal aspect),
- Incentivising citizens (societal aspect),
- Implementing a consistent and clear legal framework for secondary health data sharing (legal aspect),
- Simplifying consent mechanisms (legal aspect),
- Supporting interoperability through standardisation (technical aspect),
- Providing technical support to medical personnel (technical/societal aspect).

The report was under development from April to December 2023 and reflects information current as of 8 December 2023.

Introduction

In recent years, increasing access to health data has become a widely discussed topic[1]. The Covid-19 pandemic and the need for joint efforts to mitigate its fatal consequences have shown how valuable health data is to patients, doctors, researchers and medical institutions and how crucial it is to maintain a dynamic flow of information on patients' conditions between different institutions. During the pandemic, data analytics were used to track the spread of the virus and predict hotspots, as well as helping governments and health organisations allocate resources efficiently. Health data from patients provided researchers with critical insights into developing effective vaccines. What is more, real-time data on hospital capacities allowed for better management of resources and data-driven insights, which influenced the implementation of public health policies.

Collecting and repurposing health information from diverse sources unleashes opportunities to enhance healthcare services, facilitate research, expedite medical advancements, and empower individuals to oversee their physical and mental wellbeing more effectively. Access to a large amount of anonymised and aggregated health data can contribute significantly to discovering new treatments and understanding rare diseases. It can also foster innovation – training algorithms with high-quality, reliable data makes it possible to invent new systems based on artificial intelligence (AI) that can revolutionise healthcare. Using AI in diagnosing patients may help to reduce treatment costs by up to 50% while improving health outcomes by 40%[2]. Separate research found that AI exhibited superior capabilities in identifying skin cancer compared to experienced doctors. Researchers from the United States, Germany and France employed deep-learning techniques on more than 100,000 images for skin cancer identification. When comparing the AI's performance with that of 58 dermatologists from around the world, the AI outperformed the human experts[3].

At the same time, the challenges linked to the sharing of health data, particularly the distrust towards institutions managing this procedure, along with other obstacles, diminish the willingness of patients to disclose this highly valuable information. This phenomenon may be seen in countries like Poland, where citizens' attitudes toward sharing data are ambiguous and susceptible to destabilisation, particularly due to incidents such as the leakage of sensitive information. Therefore, while the report delves into the multifaceted dimensions of health data sharing, exploring ethical, legal and technological considerations, the emphasis is placed on the pivotal role of trust, particularly in the Polish context. As concluded by the author, without the foundation of trust, individuals may hesitate to participate in data-sharing initiatives, potentially hindering the possibility to develop the large datasets crucial for advancing medical research and public health strategies. Additionally, the significance of trust in institutions governing data has never been more important. This trust is crucial for establishing digital data spaces, facilitating seamless information exchange among various stakeholders and member states. Considering the recent advancements in this

[1] Open Data Institute (2021), 'Secondary use of health data in Europe'.
[2] IBM (2023), 'The benefits of AI in healthcare'.
[3] ibid

domain, fostering trust among patients and ensuring that individuals recognise the significance of sharing their health information within a collaborative framework is essential for the success of the future European Health Data Space. Building a resilient ecosystem means empowering patients as engaged contributors but also providing protective measures against potential ethical concerns and legal challenges. In essence, building a robust model rooted in patient trust is not just a necessity for the success of health data initiatives but also a demonstration of the conscientious and ethical advancement of data-sharing practices across the EU.

This report aims to intensify the inquiry into health data sharing and delve more deeply into the aspect of trust. It is organised into four main sections. The first scrutinises the current state of the secondary use of health data, emphasising the increasing importance of health data and describing existing policy initiatives aimed at broadening access to this information. The section on the citizens' perception explores the complexities of health data sharing in Poland, referring to the correlation between trust and a broader rule of law crisis, impacting citizens' hesitancy to share confidential information, particularly exacerbated by digital surveillance concerns. The third section includes an analysis of the legal, technical and sociocultural factors that negatively influence the health data-sharing process. Building upon the preceding section, the final part of the report offers recommendations to address previously identified challenges, including trust issues, regulatory hurdles, and insufficient digital literacy among patients and medical staff. Its aim aligns with the overarching objective of the paper, which is to furnish policymakers, healthcare institutions, and technology enthusiasts with a comprehensive analysis of potential solutions to overcome the barriers hindering health data sharing.

Towards common secondary use of health data

The increasing importance of health data

The last few years have brought a significant change in the way medical information is generated, stored and analysed. Traditional methods of keeping health records on paper are being replaced by digital data management systems that enable quick access to information and speed up various processes. The development of new technologies, Internet of Things (IoT), AI, and data analytics affects every aspect of healthcare – from patients' condition monitoring to disease diagnosis and treatment personalisation. It was estimated that the global digital health market relying on the processing of health data will almost double in size, from EUR 16bn in 2015 to EUR 31bn in 2020[4]. The newest estimations are much larger. Latest estimates say that the revenue in this market is projected to reach around EUR 152,79bn ($170.20bn) in 2023 and show an annual growth rate (2023-2027) of 10.78%, resulting in a projected market volume of EUR 230,08bn ($256.30bn) by 2027[5].

EU policies relevant for the health data sharing

Health data plays a key role in modernising medicine and enabling cross-border cooperation, as has been confirmed by the European Commission in the European Strategy for Data issued in 2020. In this document, the commission announced plans to build European data spaces, including the European Health Data Space (the EHDS)[6]. The legislative initiative on the EHDS is complementary to the Data Governance Act[7] and the Data Act[8], but it includes measures dedicated to the health sector. It also supplements the provisions of the General Data Protection Regulation (GDPR)[9] for the health-specific area. The main objective of the

---

[4] European Commission (2022), 'Impact Assessment Report Accompanying the Document Proposal For A Regulation Of The European Parliament And Of The Council on the European Health Data Space'.

[5] Statista (2023), 'Digital Health - Worldwide'.

[6] European Commission (2022), 'Proposal For A Regulation Of The European Parliament And Of The Council On The European Health Data Space'.

[7] European Commission (2022), '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)'.

[8] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules On Fair Access To And Use Of Data (Data Act)'.

[9] European Commission (2016), 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

European Strategy for Data is to create a single European market for data by enabling easy and secure access to various kinds of data. The second policy priority mentioned above, the EHDS, focuses on creating an ecosystem that empowers individuals through digital access to their personal health data (both on the national level and EU-wide); fostering a single market for electronic health systems, medical devices and high-risk AI systems; providing a trustworthy set-up for the secondary use of health data (i.e. research, innovation, policymaking and regulatory activities). The goal is also to harmonise practices for data sharing and protection within the EU and to unify the standard formats used in healthcare in different countries. The ecosystem will be built on the GDPR and the NIS 2 Directive, and will comprise of rules, common standards and practices, infrastructures and a governance framework.

Heading towards common secondary use of health data – the Polish context

At the same time, it should be noted that not all member states are ready to implement the solutions the EHDS regulation proposal brings. While countries like Finland and the UK can be considered leaders in health data reuse, in general there are a limited number of governments investing in health-systems transformation, updating their data registries, and introducing secondary use of health data policies and guidelines[10]. Poland has some policy initiatives designed to enable secondary health data sharing. However these policies are not advanced yet. The Ministry of Health and the body responsible for e-health coordination (e-Health Centre; CeZ) have jointly tried to modernise and digitalise health services, introducing, for instance, online doctor consultations or interoperable electronic healthcare records (EHR). One of the key objectives of CeZ's strategy for years 2023-2027[11] is to support data-based decision making in the health sector. It refers to the further development of a so-called 'health data warehouse' and to creating an environment that ensures smooth and secure access to data, allowing for AI and ML predictive models training. As a specific objective, CeZ indicates increasing the use of advanced methods of data analysis and establishing the Integrated Analytical Model (the IAM)[12]. The aims of this system are to place health data in one common environment; ensure a high quality of data; standardise data; and develop consistent definitions. The planned evolution of this health information database is organised into three stages, with the final stage encompassing the integration, processing, and secondary use of health data directly obtained from medical devices or personal devices.

---

data, and repealing Directive 95/46/EC (General Data Protection Regulation)'.

[10] Open Data Institute (2021), 'Secondary use of health data in Europe'.

[11] Centrum e-Zdrowia (2023), 'Strategia Centrum e-Zdrowia na lata 2023-2024'.

[12] Klinger K., Wittenberg A., 'Kikosicki: Sztuczna inteligencja ma pomóc, a nie zastąpić lekarzy [WYWIAD]', Dziennik Gazeta Prawna.

Citizens' perception of sharing health data

Importance of keeping people in the loop

Whereas plans included in the e-Health Centre strategy are ambitious and quite comprehensive, the concrete steps concerning the creation of the IAM do not mention any forms of keeping citizens in the loop. Such an approach may consequently hamper initiatives aiming at building an integrated system for health data sharing. According to the TEHDAS study assessing citizens' perception of sharing health data for secondary use, people like to be given the possibility for meaningful and active decision making in terms of the secondary use of their health data[13]. At the same time, it is important to highlight that providing a sense of control is particularly crucial in nations like Poland, where citizens exhibit a significant lack of trust in their government (as indicated by the OECD's studies, which reveal that Poles have one of the lowest levels of trust in their own government among the 38 countries analysed)[14].

The relationship between the rule of law, citizens' trust in the government, and the willingness to share data

This lack of trust among Poles should not be surprising, considering that a pivotal factor influencing confidence in institutions is the level of the rule of law in a country[15]. In Poland, this foundational value upon which the EU is based has been compromised since 2015, when democracy and the protection of human rights were jeopardised by the Constitutional Crisis[16] and the increased control over Poland's judicial system[17]. This crisis, combined with additional scandals involving the digital surveillance of Poles - such as the government's use of Pegasus spyware[18] - has resulted in individuals being cautious about sharing confidential information with public institutions. This hesitancy stemmed from the concern that data may be processed inappropriately, and subsequently used against the individuals.

---

[13] TEHDAS (2023), 'Qualitative study to assess citizens' perception of sharing health data for secondary use and recommendations on how to engage citizens in the EHDS'.

[14] OECD (2022), 'Trust in government'.

[15] Postema, Gerald J. (2019), 'Trust, Distrust, and the Rule of Law'.

[16] Szuleka M., Wolny M., Szwed M. (2016), 'The constitutional crisis in Poland 2015-2016', Helsinki Foundation for Human Rights.

[17] Gregorczyk-Abram S. (2018), 'Poland's government is undermining the rule of law'.

[18] Ptak A. (2023), 'Senate commission finds Polish government's use of Pegasus spyware to be illegal', Notes From Poland.

The Polish citizens' reluctance to share personal data with public authorities became especially evident in 2020, when public opinion resisted new regulations proposed by the Ministry of Health. The aim of this legislative initiative was to establish the digital medical information system requiring all entities providing medical services to enter data on various medical events (including pregnancy). Whereas the grounds for the proposal were legitimate (creation of the new system was based on the recommendations of the European Commission), due to the local context and the issues related to the abortion ban, people presumed that the regulation was aiming to exercise control over Polish women[19]. As Marta Musidłowska, an expert from KU Leuven, explained in an interview conducted for this research paper:

> *"Within three years [of the outbreak of the pandemic], the number of people willing to share health data has increased by approximately 27% [according to the Polish Economic Institute]. However, the lack of trust in the government, possibly stemming from the crisis of the rule of law in Poland and amendments to the abortion law, has led to controversies surrounding legislative initiatives. Even those derived from EU law, which should uniformly affect all member states, could have become sources of contention in Poland and contribute to widespread disinformation.*

In the last few years, public trust in the healthcare system in Poland has been one of the lowest in the EU[20]. Whereas this refers to traditional healthcare, the citizen's approach toward sharing their data seems to be ambiguous. According to the Polish Economic Institute's (PIE) study, in 2020 Poles were not willing to share their personal data – not even half of respondents (45.2%) were eager to share data on their health habits for the needs of a public prevention programme and only 39.5% wanted to share information about their general health condition[21]. When it comes to general citizens' approach to data privacy, the level of concern

[19] Posner, L., (2022), 'Poland's New 'Pregnancy Registry' Raises Red Flags; Some Polish women feel their privacy and autonomy are on the line', Think Global Health.

[20] Masterson, V. (2020), 'These are the countries that have the greatest trust in their health services', World Economic Forum.

[21] Grzeszak, J., Śliwowski, P., Święcicki, I., & Wincewicz-Price, A. (2020), 'Czy chcemy dzielić się prywatnymi danymi?', Polski Instytut Ekonomiczny.

about data theft and security breaches remains high among Poles. At the same time, the possibility of obtaining benefits resulting from sharing data significantly changes the perspective – more than half of respondents would be willing to provide data to facilitate online shopping (56%), receive personalised recommendations (55%), or recommendations of new products (52%)[22]. This dualism in the way people perceive their private data has been noticed by Ligia Kornowska, Managing Director of the Polish Hospital Federation, leader of AI Coalition in Healthcare for Poland, and Chair of the Board of Donate your Data Foundation and Data Lake. When asked about citizens' approach to secondary use of their health data, Ligia Kornowska responded that:

> *It is quite ambiguous. Some citizens are concerned about the security of their data, while deliberately sharing elements of their medical records on social media platforms. However, in the experience of the Donate your Data Foundation educators, patients are very willing to share their medical data if they understand what it entails and have the possibility to control it.*

Evolution of public attitudes toward health data sharing in Poland: Insights from 2020 to 2023

The beginning of the Covid-19 pandemic did not bring a considerable change in the willingness of Poles to share their data, which has been confirmed by resistance to use the Stop Covid ProteGO Safe application – a device compiling data on citizens and Covid-19. This hesitancy of Polish citizens was confirmed in a study in which less than 30% of respondents declared that they would provide private data to improve health care services - in the Netherlands and Sweden, the respective number was around 80%[23]. However, in 2023, the PIE's study on the willingness of Poles to share their data was repeated and presented findings significantly different from those from 2020. According to the recently conducted research, 70% of respondents declared their willingness to share their data on health, energy use or consumption if they were assured that such data will be used in the public interest.[24] Meanwhile, 68% of survey participants declared they would share their health data for purposes related to development of a preventive programme against lifestyle diseases. Compared to the PIE's study from 2020, the

[22] Olak R. (2023), 'Badanie EY: Polacy obawiają się kradzieży danych, ale chętnie je udostępniają, jeśli generuje to korzyści', EY.
[23] Duszczyk M. (2021), 'Polacy nie chcą dzielić się prywatnymi danymi z państwem', Rzeczpospolita.
[24] Nowakowski, W., Święcicki, I. (2023), 'Czy Polacy chętnie dzielą się prywatnymi danymi?', Polski Instytut Ekonomiczny.

number of the respondents willing to share their health data for secondary use increased by 22.8 percentage points. The authors, however, underline that while the general approach to the study was similar, there were some differences in the wording of individual questions and therefore a direct comparison of the results is not possible. Nonetheless, the PIE's experts indicate that apart from methodological considerations, the change in citizens' attitudes towards data sharing might have resulted from various factors such as the experience of the three-year Covid-19 pandemic or increased technological literacy. The first has undoubtedly raised awareness of the importance of information exchange in healthcare. The second might have given people a sense of control over data, which is crucial in the case of sharing sensitive data - compared to the survey from 2023, the percentage of respondents declaring their ability to control their data increased by approximately 27 percentage points[25].

An interesting finding from the PIE's report from 2023 is that 55.8% of respondents believe that the Ministry of Health should be able to access data from sport and fitness applications in order to develop and implement prevention programmes (this is 19.3 percentage points higher than the one from 2020). These statistics find confirmation in the study on Poles' approach toward new technologies, in which, next to banks, medical institutions and doctors enjoy the greatest trust when it comes to data security[26]. As Ignacy Święcicki, Head of the Digital Economy Department at the Polish Economic Institute outlined in the interview carried out for this project:

> *"Studies from Poland and abroad show that trust in a given institution is crucial – hence the discrepancies between the willingness to share data with a doctor or a research institute and a pharmaceutical company. According to the PIE's study, in the case of health data, the difference between the respondents' willingness to use a public and private application - in favour of the public one - was the biggest - even though not very significant. However, it should be taken into account that in the period preceding the study, there were no incidents publicised in the media related to*

[25]Nowakowski, W., Święcicki, I. (2023), 'Czy Polacy chętnie dzielą się prywatnymi danymi?', Polski Instytut Ekonomiczny.
[26] Minds & Roses (2023), 'Polacy chcą mieć kontrolę nad technologią – badanie ING'.

major leaks and theft of personal data concerning the Ministry of Health.

Barriers to health data sharing: the lack of trust and other significant obstacles

Fragile trust: the potential impact of mishandling health data on public confidence (societal obstacle)

The shift to a more positive attitude toward sharing health data should be considered as an opportunity to develop and introduce data-driven innovations in the public sphere and build common confidence in such measures. However, despite the certain reliability of the healthcare service providers, distrust toward public institutions in Poland in general remains an obstacle. According to the Policy Institute from King's College study, 75% of Poles think the government does not communicate accurate and unbiased information[27]. What is more, in Poland there is a negative view of the truthfulness and rightfulness of the government - with 70% of the respondents believing the country's government is not honest and trustworthy[28].

Recent events involving the Polish Ministry of Health might have eroded citizens' trust in the secure and respectful handling of data by public institutions. In August 2023, the Polish Health Minister's disclosure of sensitive information about a doctor's prescribed medication, following this doctor's public criticism of the Ministry of Health, triggered public outrage[29]. This act was perceived as retaliation and raised concerns about the security and respect for citizens' data held by public institutions. The minister's actions were condemned by both the medical and legal communities, leading to notifications to the prosecutor's office regarding suspected crimes of exceeding authority and breaching the right to the legal protection of private life. Doubts about the security of the public IT systems were further raised soon after, when a Polish broadcaster (TVN) reporter discovered that the system for e-prescriptions is not sufficiently confidential. It was the case that any doctor knowing any patient's PESEL number (Universal Electronic System for Registration of the Population) could access the government site gabinet.gov.pl and check the history of prescribed medicines to a patient. This function was switched off after the information was made public, and many organisations, including the Supreme Medical Council, stated that looking into non-anonymised health data without patients' knowledge raises justified concerns

[27] The Policy Institute, King's College London (2022), 'Public attitudes towards national government and other institutions'.
[28] ibid
[29] Ptak A. (2023), 'Poland's health minister sparks outrage after revealing sensitive information about doctor', Notes From Poland.

regarding the potential for data breaches[30].

As already mentioned, recent events, combined with the rule of law challenges, may result in people feeling sceptical about sharing sensitive information about their health condition and accepting the secondary use of their health data. This shows that beyond legal and technical challenges, socio-cultural factors are pivotal in constructing health data ecosystems. Therefore having in force appropriate safeguards protecting the individuals, providing democratic governance over the process of data sharing, and ensuring accountability of public institutions, is crucial for the successful and secure sharing of health data.

Lack of awareness or digital literacy (societal obstacle)

A lack of awareness regarding data sharing remains an issue. A number of interviewees spoke about individuals not being familiar with the potential benefits that can arise from sharing their health data, such as contributing to medical research, improving public health initiatives, and enabling more personalised healthcare services. This lack of awareness refers to individuals not realising the broader societal implications of health data sharing but also being concerned about privacy and security. According to Recital 49 of the EHDS, health data should be anonymised, or at least pseudonymised, with the encryption key held exclusively by a health data access body to reduce risks to the right to privacy. However, people may not understand methods of securing data and they might not be aware of what particular notions actually mean. As a consequence, patients' fear of their data being misused may result in deepening their reluctance to share it. Without a clear understanding of how their data could be utilised for the greater good and how it can be secured, people may be hesitant to engage in health data sharing initiatives, leading to missed opportunities for advancements in medical knowledge and innovative therapies.

Regulatory barriers (legal obstacle)

The EU's GDPR, in spite of harmonising data protection laws and providing greater protection of individuals, also introduced barriers to health data sharing. Different member states interpret GDPR in softer or stricter ways and there are discrepancies in implementation of the GDPR into national regulations[31]. According to the TEHDAS report, the legal barriers resulting from misinterpretation, or misalignment of the GDPR are among the most burdensome in the case of the secondary use of data. Inconsistent interpretation led to a fragmentation of approach to data privacy in the EU[32]. Certain ambiguities in applying GDPR to health data are also visible in Poland. This has become particularly apparent during works on digital healthcare innovations, such as, for instance, telemedicine solutions[33]. Moreover, there are quite large definitional discrepancies in the Polish regulations applicable particularly to health data

[30] Górski M. (2023), 'E-recepty a cyberbezpieczeństwo', Ministerstwo Zdrowia. odpowiada', cyberdefence24.pl.
[31]Vukovic, J., Ivankovic, D., Habl, C. et al. (2022),' Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective'.
[32]TEHDAS (2022), 'Report on secondary use of health data through European case studies'.
[33]Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie społecznym', Okręgowa Izba Lekarska w Warszawie.

sharing, for example with medical documentation, health data or encrypted data[34].

In the case of health data, Article 9 of the GDPR sets legal grounds for data processing. Whereas explicit consent is one way to legitimise processing special category personal data, Article 9(2) lists nine other conditions - e.g. processing for the purposes of preventive or occupational medicine. The alternative options for health data sharing are generally more restrictive and tailored to particular situations. Apart from the regulation on data privacy, Poland has specific legislation on the processing of health data for planning, management, administration and improvement of its health and care system entities, such as health authorities[35]. The grounds for sharing health data in this case is Art. 26 of the Act on the Patient's Rights and the Patient's Rights Ombudsman[36], which contains a list of those entitled to obtain access to medical data - for instance, the National Health Fund; medical self-government bodies and health consultants; the Medical Research Agency. At the same time, the legislation on the re-use of health data that were collected initially in the context of providing care, but which may later be re-used, is quite limited[37]. What seems to be clear is that the current legislation in Poland - unlike in Switzerland, Belgium or the UK - does not facilitate secondary use of health data, and is focused primarily on the protection of privacy [38]. This overly risk-averse approach in applying the GDPR by healthcare institutions results in rejecting requests for health data, even if legal and ethical conditions are met[39]. To realise the value of health data, combatting the persisting misunderstanding that sharing data cannot be fully compatible with the goal of protecting sensitive data is crucial. In the EU countries where the overly risk-averse approach is less prominent, the GDPR is interpreted in a way that allows reuse of anonymised health data for research, diagnostic and personalised healthcare purposes. For instance, the Finnish Social and Health Data Permit Authority Findata[40] demonstrates that it is possible to introduce adequate policies and design models for secondary health data sharing that ensure effectiveness while guaranteeing privacy protection.

Lack of proper infrastructure for the secondary use of data (technical obstacle)

The importance of building a digital healthcare information system was marked in the Ministry of Health's 'Policy Paper for health care sector 2014-2020' and further underlined in the strategic document 'Healthy Future 2021-2027'[41]. As a result of the actions taken on the national level, the e-Health platform[42] has been

[34] Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie społecznym', Okręgowa Izba Lekarska w Warszawie.
[35] European Commission (2021), 'Country fiches for all EU MS Annex to the study 'Assessment of the EU Member States' rules on health data in the light of GDPR'.
[36] Gov.pl, 'Act on the Patient's Rights and the Patient's Rights Ombudsman'.
[37] European Commission (2021), 'Country fiches for all EU MS Annex to the study 'Assessment of the EU Member States' rules on health data in the light of GDPR'.
[38] Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie społecznym', Okręgowa Izba Lekarska w Warszawie.
[39] TEHDAS (2021), 'Summary of results: case studies on barriers to cross-border sharing of health data for secondary use'.
[40] Findata, https://findata.fi/en/
[41] Ministry of Health (2021), 'Zdrowa Przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021-2027, z perspektywą do 2030'.
[42] Ezdrowie, https://ezdrowie.gov.pl/

established as part of the project named 'Electronic platform for collecting, analysing and sharing digital resources about medical events'. Through this platform, digital services in the health sector have been introduced – e-prescriptions (January 2020), e-referrals (January 2021) and the app that enables doctors to provide teleconsultations, fill out the e-Vaccination Card, and issue e-sick leave. Since the Internet Patient Account (IKP) and the mobile application were launched in May 2021, patients have had access to their medical data and documents online.

At the same time, in Poland, the vision of using data infrastructure beyond interoperable electronic health records is considered as limited[43]. The new e-Health Center strategy for 2023-2027 includes plans for participating in European e-health projects - including EHDS - increasing access to data for healthcare institutions and external stakeholders - the scientific community and other entities - and eventually integrating, processing and re-using data. However, despite the ambitious plans, experts say that the current infrastructure might not be resilient and mature enough to allow the secondary use of such sensitive data as health data. Therefore, concerns around maintaining the security of health data remain an obstacle. Undoubtedly, developing systems for managing sensitive data security is technically more demanding than, for instance, industrial data[44]. And even if the system is designed in a way that ensures resilience and security, it may still be prone to cyber-attacks or the hacking of digital infrastructure. What is more, there is a risk related to the possibility of an entity accessing and using health data without the patient's knowledge or consent. This could lead to a leak of extremely sensitive information, which could be detrimental not only for the patient, but for the whole society - as it would undermine trust in the digitalisation of healthcare.

Interoperability and standardisation issues (technical obstacle)

Data interoperability remains one of the greatest challenges in the health data ecosystem[45]. According to the study on the 'Interoperability of Electronic Health Records in the EU', conducted for the European Commission, Poland, Cyprus, Germany, Ireland, Luxembourg, and Romania all show an overall low level of use across all EHR data types[46]. What is more, in Poland, interoperability is considered weak, as if there is any, it occurs only within the same sector. Moreover, Poland has not yet managed to unify standards related to the digitisation of healthcare records[47]. The reasons for the insufficient interoperability and low level of use of electronic health records in Poland can be characterised as a lack of proper standardisation and impaired dataflows between private and public entities.Since there is no one unique patient profile and it is not possible to access the records of a patient who uses public and private services at the same time[48].

---

[43] Open Data Institute (2021), 'Secondary use of health data in Europe'.
[44] Musidłowska M., Wawrzyniak B., Zygmuntowski J.J. (2022) 'Unleashing the potential of data. Managing data as a shared resource'.
[45] Open Data Institute (2021), 'Secondary use of health data in Europe'.
[46] European Commission (2021),'eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU Lot 1 – Interoperability of Electronic Health Records in the EU'.
[47]Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie społecznym', Okręgowa Izba Lekarska w Warszawie.
[48]Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie

How to support initiatives such as the EHDS on the national level and engage citizens in data-sharing

The European Health Data Space represents a visionary stride towards harnessing data for the betterment of healthcare across the EU. As pointed out in this report, supporting health data sharing on the national level and tackling the issues resulting from a delicate interplay between societal concerns, legal framework, and technological infrastructure is crucial for the EHDS initiative to succeed. This section casts a spotlight on the main pillars that are essential for health data sharing, presents specific areas of intervention, and outlines actions that should be taken to facilitate the introduction of the EHDS across societal, legal and technical aspects.

By elaborating on the identified barriers and presenting a roadmap for overcoming them, this part of the report aims to provide a comprehensive analysis of aspects that should be tackled to pave the way towards a unified health data space that serves the collective good.

Societal aspects

In the dynamic landscape of healthcare, unlocking the potential of health data is crucial to advancing medical research, improving public health and tailoring healthcare services. However, numerous societal barriers impede the seamless sharing of health data, hindering the realisation of these transformative processes. Key among these barriers are the lack of trust and widespread poor awareness of the numerous benefits that result from responsible data-sharing practices discussed earlier. If we acknowledge these challenges as critical obstacles, the following actions emerge as essential pathways for overcoming societal impediments:

- establishing trust through the proper design and democratic governance of data-sharing models,
- launching an extensive awareness campaign among citizens, and
- introducing incentives to promote active participation in the data-sharing initiatives.

społecznym', Okręgowa Izba Lekarska w Warszawie.

Through an in-depth exploration of these societal dimensions, this section endeavours to investigate effective approaches in dismantling barriers, fostering a health data sharing ecosystem that is more transparent, informed and collaborative.

Building trust through design and democratic governance of the data-sharing models

'Public opinions and behaviour around health data in the GDPR era', a report from 2018, confirmed that people are more concerned about the privacy of health data than other types of personal data[49]. This might be an explanation of why, in the case of patients' data, trust is such an important factor for successful data sharing [50]. It comes as no surprise that in member states where transparency and trust in public institutions is considerably high, the models for the secondary use of health data thrive. Finland, where citizens declare very high confidence levels in public authorities[51], is a pioneer in the secondary use of health data and digital innovation in medicine. Similarly, in Denmark, where people believe in the integrity and resilience of the system, data is seen as a common good, and its re-use receives widespread support from citizens[52]. Therefore, the first step, to convince citizens to share their health data for purposes other than receiving medical care, is important to build societal trust in the new data-sharing models.

The EHDS legislative proposal creates a chance to 'level the playing field' between member states in terms of access to health data and to drive research and innovation across all EU countries. It also aims to integrate public engagement in health data-sharing through the decentralised EU infrastructure. However, in this case, citizens' involvement in the process seems to be limited. While the EHDS aims to empower citizens through measures such as granting them access to their health data and control over which healthcare professionals can access these records, the emphasis on citizen empowerment in not that pronounced in the context of secondary data use[53]. What is more, the EHDS does not say much about collective governance of the process of sharing health data, which, according to the literature on the common data spaces, should be ensured through participation and democratic oversight[54]. Involving various stakeholders in the governance processes helps to ensure that the system is more transparent and accountable and includes a wide range of voices in its operation and oversight. Engaging the public in establishing and governing health data-sharing models ensures transparency, which helps alleviate concerns about data misuse.

---

[49] Data Saves Lives, 'Public opinions and behaviour around health data in the GDPR era'.
[50] Bowden C., Devaney S., The Guardian (2023), 'Trust is the key to healthcare data sharing' .
[51]Sitra (2019),'A Finnish Model For The Secure And Effective Use Of Data Innovating And Promoting The Secondary Use Of Social And Health Data'.
[52]TEHDAS (2022), 'Country visit – Denmark'.
[53]Saelaert M., Mathieu L., Van Hoof W., Devleesschauwer B., (2023), 'Expanding citizen engagement in the secondary use of health data: an opportunity for national health data access bodies to realise the intentions of the European Health Data Space'.
[54]Tarkowski A., Zygmuntowski J.J., Open Future (2022), 'Data Commons Primer Democratizing The Information Society'.

This, consequently, fosters greater trust among citizens in the data-sharing scheme, increasing their willingness to participate. It also reassures them that their data is being used responsibly and for the collective benefit of society.

In terms of the secondary use of health data and citizens' participation, the EHDS includes plans to create and connect institutions responsible for managing health data reuse in all member states[55]. These Health Data Access Bodies (HDABs) will be crucial for maintaining a secure and trustworthy ecosystem for data sharing for secondary use and, therefore, should aim for a high level of transparency and public engagement. Citizens should be properly informed about how their health data is utilised, and HDABs should strive for a significant degree of transparency, especially in their communication with patients. At the same time, while the EHDS imposes the obligation for the member states to inform the public at large (Article 38 (4)) about the benefits deriving from the existence of HDABs, it lacks other trust-enhancing measures in HDABs' design. Moreover, the current version of the EHDS gives the member states a wide margin of discretion in how they designate HDABs. This, however, may raise citizens' concerns regarding the political independence of such institutions. Although article 36(3) stipulates that HDABs shall not be bound by any instructions when making their decisions, the regulation does not seem to provide any additional trust-by-design mechanisms. This, however, may pose a risk of overreaching powers by the authorities and influencing HDABs' operations. Therefore, to build citizens' trust in the EHDS, it is crucial to provide a resilient regulatory framework granting the European Commission with sufficient tools to execute its competencies but also allowing societal control over the functioning of HDABs.

Whereas the currently proposed text of the EHDS regulation mentions the need to maintain "cooperation with stakeholders' representatives, especially with representatives of patients, data holders and data users"[56], it does not allow data subjects to actually contribute to the HDABs' work and decision-making. To maximise public trust in data spaces, it is essential to guarantee that citizens are well-represented and may control the process of data re-use. While invoking HDABs on the national level, it is crucial to consider two important actions: first, broadening the scope of citizen engagement to encompass secondary data use, and second, acknowledging and facilitating a wide range of citizen involvement. Democratic participation could be introduced through such measures as supervisory councils, citizen panels, and assemblies[57]. Various forms of patient representation would ensure the flow of information between HDABs and society and offer the chance to influence decisions on important matters related to secondary health data sharing.

Raising citizens' awareness

Even if people are aware of the value of their data, they do not always notice the immediate benefits resulting from sharing it. Therefore, it is important to raise citizens' awareness on the topic and facilitate public discourse with examples of good practices in the field of data sharing, benefits of data reuse, and methods

[55] Cyber Risk GmbH (n.d.) 'European Health Data Space'.
[56] European Commission (2022), 'Proposal For A Regulation Of The European Parliament And Of The Council On The European Health Data Space'.
[57] Musidłowska M.,Vogelezang F., Wawrzyniak B., Open Future, Instrat (2022) 'Feedback on the Proposal for a Regulation on the European Health Data Space'.

that ensure privacy for personal information. Ligia Kornowska, Chair of the Board of Donate your Data Foundation and Data Lake, pointed out:

> *With the current level of technological development, we are able to provide citizens with the tools to control how their data is processed. Not only should we be asking patients for their trust, but we should also allow them to be in control. Accessing data by untitled entities or persons can be very dangerous for society as a whole. This is why we need to develop a culture of openness and transparency.*

To increase citizens' awareness of the advantages of health data sharing, it is crucial to use a multifaceted approach. First, public discourse should be facilitated with campaigns on health data sharing. Such campaigns should be carried out jointly by experts in the fields of digitalisation and innovation in healthcare, to give these promotional activities credibility. As Ignacy Święcicki from the PIE underlines:

> *Proper communication initiatives seem to be crucial to incentivise citizens. The effectiveness of a communication strategy depends on the content of the message, the role of the entity, the context, the complexity of the information, and the initiator of the communication. It is a good idea to engage people who enjoy authority among citizens, who are popular in various social groups - such as social leaders and scientists - and use communication channels that allow you to reach a wide range of recipients.*

Moreover, it is important to undertake educational initiatives to increase digital literacy and inform individuals about the positive outcomes of data sharing. These actions should emphasise how sharing health data can lead to more personalised medical treatments, faster responses to public health crises, and the development of innovative healthcare solutions.

Secondly, it is important to provide patients with a clear explanation of the data-sharing process, as well as the methods that guarantee privacy and security. Making citizens more knowledgeable about the rules governing health data reuse and the technologies in place could be achieved by opening various educational programmes. A good example of such practice is cooperation between the public and private sectors in Estonia, where companies paid to train citizens on how to use digital banking systems. Promoting eBanking and educating people in this field has helped establish a new tech era in Estonia, creating new business opportunities.[58] Another example of cooperation between different stakeholders aiming at increasing awareness and building mutual understanding is the activity of Understanding Patient Data (UPD), a UK organisation hosted by the NHS Confederation that works as a bridge between policymakers and patients. The organisation is committed to furnishing unbiased insights into the utilisation of patient data while representing the perspectives of patients and the general public to policymakers and data custodians.

The responsibility of educating patients relies on healthcare providers and institutions, as well as physicians. According to a European Consumer Organisation (BEUC) study, willingness to share health data depends on the level of proximity and trust toward the receiving entity. Most people declare eagerness to give access to data to their general practitioner for care purposes (88%). Accordingly, the most trusted category of health professionals are those whom patients engage in regular contact with – and more than half (54%) of respondents declared high trust in them[59]. Therefore, it could be useful to educate primary care physicians and encourage them to actively engage with patients, sharing success stories and real-world examples of how data sharing has directly improved healthcare outcomes. By promoting a culture of openness, trust and education, citizens could see better the advantages of health data sharing and actively support initiatives related to its implementation.

Incentivising citizens

Incentivising individuals to share their health data is essential for the health data-sharing models to succeed. What may help promote sharing health data for purposes other than secondary use is offering certain benefits - tangible or intangible - to individuals. These benefits can take the form of financial incentives, such as reduced healthcare costs or access to more advanced and better profiled treatments. A good example of how the initiative directly engages with the citizens is the Polish foundation Donate Your Data (Fundacja Podaruj Dane)[60], which has created a data donation system to address the issues related to obtaining patients' medical data for scientific research.

---

[58] Widén S., Haseltine W.A. (2015), 'Case Study: The Estonian eHealth and eGovernance System'.
[59] BEUC (2023), 'Consumer attitudes to health data sharing Survey results from eight EU countries'.
[60] Fundacja Podaruj Dane https://podarujdane.pl/

The system provides anonymity (collects only anonymised data) security (relies on blockchain technology (trust and control) participants can control their data and withdraw their consent at any time. What is more, individuals receive certain benefits for contributing to the project. The Chair of the Board Donate your Data Foundation and Data Lake, Ligia Kornowska indicates that data donation is similar to blood donation:

> *When patients donate blood, they get a chocolate bar, discounts on public transport and a day off. When patients share their data for R&D purposes through the Donate Data Foundation, they get health-promoting benefits: discounts on medical examinations, vitamin drinks and glasses. We think this is not only a good way to reward patients for being honorary data donors, but to encourage them to strengthen their preventive activities and habits.*

Legal aspects

The legal environment surrounding health data sharing reveals myriad challenges, with inconsistent interpretations of the GDPR across member states and an overarching risk-averse approach introduced by the GDPR itself serving as prominent barriers. The lack of clarity in interpreting the GDPR introduces complexity and uncertainty, while the GDPR's cautious stance poses challenges for the introduction of measures to allow health data to flow more freely. To surmount legal challenges, two primary recommendations take centre stage: instituting a consistent and transparent legal framework for secondary health data sharing and streamlining the consent mechanism - if consent is needed. This section strives to address legal obstacles by identifying effective strategies for creating a unified and practical legal framework that promotes responsible and secure practices in health data sharing.

Implementing consistent and clear legal framework for secondary health data sharing

To overcome challenges deriving from misinterpretation or misalignment of the GDPR, as well as the fragmentation of national legislations on secondary data sharing, the European Commission proposed The European Health Data Space Regulation (EHDS). This comprehensive legislative act provides a framework for

finding a proper balance between protecting patient privacy and enabling responsible data sharing. Solutions that are expected to address current legal challenges for secondary health data sharing include[61]:

- **aligning rules and principles for data governance, data protection and security standards** – ensuring that health data sharing is conducted in a manner consistent primarily with the GDPR, as well as the Regulation (EU) 2017/745 on medical devices (Medical Devices Regulation) and the Regulation (EU) 2017/746 on in vitro diagnostics medical devices (In Vitro Diagnostics Regulation), the proposed Artificial Intelligence Act, the proposed Data Governance Act and the proposed Data Act, as well as the Directive 2016/1148 on security of network and information systems (NIS Directive) and the CBHC Directive;
- **ensuring consistent application of the regulation throughout the European Union** – for that purpose, the Health Data Access Bodies should cooperate with each other and with the commission, as well as with stakeholders, including patient organisations;
- **introducing strong mechanisms to safeguard against abuse** – for instance, lists of permitted uses of electronic health data processed for secondary use (Art. 34) and prohibited uses (Art. 35), as well as rules for governance and practical mechanisms;
- **promoting transparency in data processing and accountability mechanisms** – ensuring that data-sharing initiatives are conducted with integrity and under clear legal obligations.

Simplifying the consent mechanism

Most actions these days require 'opting in' to a behaviour. Nonetheless, choosing an 'opt-out' model as a default has impacted numerous individual behaviours, such as participating in retirement savings schemes, becoming an organ donor, and contributing to vaccination rates.[62] The importance of behavioural economics to the design of the data-sharing process has been underlined by Ignacy Święcicki from the PIE:

> *What could be helpful for initiatives such as secondary health data sharing is simplifying the data transfer process, using clear communication, implementing default settings in health data applications, etc. Also, approach to data collection matters – verifying if there are any default settings available, how easily a person can issue consent for data reuse;*

[61] European Commission (2022), 'Proposal For A Regulation Of The European Parliament And Of The Council On The European Health Data Space'.
[62] Jhaveri R. (2021), 'Big Data and Behavioral Economics in Infectious Diseases'.

opt-out is not always a good solution, but maybe if the data were analysed legally and kept secure, only few people would opt out.

Whereas in some countries, the opt-out approach is already in force - e.g. an opt-out system for tissue research in Belgium, for the collection of personal health data in registries in France, or the "national data opt-out" in the United Kingdom[63] - the sharing-by-default model often invokes controversies. For instance, in the UK, citizens voiced concerns about the opt-out scheme, expressing dissatisfaction with decisions being made about them without consultation[64]. This sentiment - combined with the lack of trust in the government - consequently led to a backlash, which resulted in millions of people opting out of the data-sharing scheme[65]. At the same time, studies have shown that opting out may be preferable to seeking consent for every personal data use - as it burdens patients disproportionately - and an opt-in approach - which leads to a less representative study population[66]. Nevertheless, the UK's example highlights that the success of the opt-out model also depends on citizens' trust in the entire system and the presence of proper safeguards.

The original legislative proposal for the EHDS did not provide provisions for a consent mechanism for the secondary use besides referring to the national law (Art. 33). This is because data for secondary use is either anonymised or pseudonymised, and there are strong mechanisms safeguarding people against abuses - including lists of permitted (Art. 34) and prohibited (Art. 35) uses, as well as rules for governance and practical mechanisms. However, in the Draft ENVI-LIBE Report of 10 February 2023,[67] an opt-out option was introduced as a measure to better respect the right of citizens and patients to control access to their data. Discussion continued on whether to include an opt-in/opt-out option or not to mention the consent mechanism. Some European stakeholders expressed concerns that implementing any opt-in or opt-out mechanism could pose a genuine risk of incorporating data bias into the EHDS and lead to data disparities, where datasets underrepresent certain segments of the overall population[68]. At the same time, civil society and consumer organisations have been underlining that an

---

[63] Verhoeven E. , Kroneman M. , Wilson P., et al. European Commission (2021), 'Country fiches for all EU MS Annex to the study 'Assessment of the EU Member States' rules on health data in the light of GDPR'..

[64] Sterckx S., Rakic V., Cockbain J., Borry P. (2015), '"You hoped we would sleep walk into accepting the collection of our data": controversies surrounding the UK care.data scheme and their wider relevance for biomedical research'.

[65] Jayanetti J., The Guardian (2021), 'NHS data grab on hold as millions opt out'.

[66] National Data Guardian for Health and Care (2016), 'Review of Data Security, Consent and Opt-Outs', and Henshall, C., Potts, J., Walker, S., et al. (2020), 'Informing National Health Service patients about participation in clinical research: A comparison of opt-in and opt-out approaches across the United Kingdom'.

[67] European Commission (2022), 'Proposal For A Regulation Of The European Parliament And Of The Council On The European Health Data Space'.

[68] Biomedical Alliance in Europe, The Digital Health Society, Eatris, DigitalEurope et al. (2023), join statement 'Enabling effective secondary use of health data in Europe: specific recommendations for a potential opt-out mechanism for the EHDS'.

easy-to-use opt-out mechanism should be considered as a minimum for patients to rely on if they do not want their data to be used for secondary purposes through the EHDS[69]. After the heated debate on the EU level, recent discussion on the Regulation agreed on a mandate to develop the initial EHDS proposal in the area of consent mechanisms, stating that member states will have the discretion to allow patients to opt out of the new data-sharing system[70]. This should be considered as a step toward making secondary health data sharing more common while building patients' trust and giving them a sense of control over their information.

Technical aspects

As explained earlier, health data sharing encounters not only societal challenges but also problematic technical barriers that demand strategic interventions. Foremost among these obstacles is the lack of proper infrastructure for the secondary use of data, combined with persistent challenges related to interoperability and standardisation. Recognising the significance of addressing these impediments, this section provides recommendations aimed at overcoming them by supporting interoperability through standardised practices and bridging the gaps that hinder data exchange between institutions and member states. Additionally, acknowledging the crucial role of medical personnel, this section explores the provision of technical support to empower healthcare professionals in navigating and using advanced data-sharing technologies.

Supporting interoperability through standardisation

Data-sharing infrastructure plays a key role in ensuring the secure and seamless exchange of health data across various actors, from doctors and healthcare institutions to research organisations and governments. Currently, technical barriers related to data standardisation, interoperability, security and the integration of diverse systems pose a significant challenge for many member states. Despite the eHealth Network recommendations to use the Electronic Health Record Exchange Format standards, the real uptake of the format is very limited, resulting in fragmentation and uneven portability of electronic health data. [71] In Poland, there is the Polish National Implementation of HL7 CDA, a formal set of rules for maintaining and storing electronic medical records issued by the Polish e-Health Centre. However, most entities do not use the unified standards recommended in the document and, instead, use one of several recording systems, such as HIS, LIS, PACS, RIS[72]. Therefore, it can be concluded that to enhance the interoperability of electronic health data, it is necessary not only to adopt common standards, but also to make them binding and compulsory. This approach has been confirmed in the public consultations on establishing the EHDS, in which the majority (67%) of the respondents stated that in the area of

[69]BEUC (2023), 'Consumer attitudes to health data sharing Survey results from eight EU countries'.
[70] European Commission (2023), 'European Health Data Space: Council agrees its position'.
[71] European Commission (2022), 'Proposal For A Regulation Of The European Parliament And Of The Council On The European Health Data Space'.
[72] Libura M., Imiela T., Głód-Śliwińska D. (2023), 'Cyfryzacja zdrowia w interesie społecznym', Okręgowa Izba Lekarska w Warszawie.

secondary use of health data, mandatory use of technical requirements and standards is crucial to facilitate interoperability and data flows between numerous stakeholders in the EU.

Providing technical support to medical personnel

The EU-funded HealthData@EU, maintained and governed by the EC, will facilitate cross-border use of health data for secondary use[73]. Therefore, it can be expected that the issues related to the lack of a proper digital infrastructure and common standardisation will be addressed - at least to some extent - together with the implementation of the EHDS and the introduction of the new platform. Nonetheless, there is a remaining issue of the lack of proper technical training of medical personnel. In Poland, despite access to the network and the possibility of using IT tools, nearly 74% of institutions surveyed in the e-Health Center study do not digitise documentation kept in paper form and only 26.1% of entities digitise paper documentation. This might be due to the lack of digital skills among healthcare personnel and very limited support from the IT specialists - more than half of the surveyed facilities do not have an internal IT support team (53.7%), while in 28% of entities, IT services are provided by medical staff[74]. Comprehensive plans for the digital transformation of the Polish health sector should, therefore, include providing resources and adopting strategies for the development of medical informatics, fostering the progress of science in this field, and, most importantly, ensuring that medical personnel receive professional IT support and have the skills and capacity to actually collect, process and share health data.

[73] European Commission (2022), 'Data sharing through eDelivery in the HealthData@EU'.
[74] Centrum e-Zdrowia (2022), VI Edycja 'Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą'.

Summary and key takeaways

Compared to other sectors, the health sector is best positioned to propose, introduce and promote measures for the secondary use of data. Not only do health institutions enjoy the greatest trust (compared to other public bodies), but citizens are also more conscious of the benefits of health data sharing. This is undoubtedly a great opportunity for policymakers to prepare the ground for the secondary use of health data and make the healthcare sector a pioneer in introducing innovative solutions based on data. Nevertheless, it seems like some member states are missing this chance. The introduction of the EHDS will undoubtedly be a complex and burdensome process. Still, it might help to level the healthcare digitalisation playing field and close the gap between those countries pioneering in health data re-use and those lagging behind.

The report reiterates the significance of health data and highlights key challenges that need to be addressed for the establishment and full functionality of a digital health data space. Examining these obstacles from the viewpoint of a citizen residing in the member state, where trust in public institutions has historically been low, the author primarily addresses societal concerns related to the sharing of health data. Given recent privacy concerns, the report places significant emphasis on addressing the uncertainties regarding shared private information and the imperative to cultivate trust through a well-designed and democratically governed data-sharing model. Notably, considering various citizens' attitudes toward national institutions across EU countries, it might pose significant challenges to introduce initiatives like the proposed EHDS regulation in member states where confidence in public authorities is low. In addition to the societal aspects, the paper sheds light on regulatory challenges associated with health data sharing. These include discrepancies in health data definitions and the dilemma of selecting a consent model for data sharing that strikes a balance between patients' rights and facilitating increased data sharing. Certain technical factors have been highlighted, as they are intricately tied to the evolution of the digital data space. These include the need to improve interoperability through standardisation and to provide better IT support to medical staff.

Addressing those barriers may pave the way for establishing a collaborative health data environment that combines rigorous legal and technical standards with societal values. The goal, therefore, is to help understand the importance of building a health data space that not only meets regulatory requirements but also aligns with society's diverse needs and expectations. However, it is crucial to acknowledge that this paper represents merely the tip of the iceberg – a concise overview of the current issues pertaining to the secondary sharing of health data. Future research efforts should focus particularly on scrutinising the EHDS regulation, exploring ways to enhance its functionality for research purposes while maintaining the confidentiality of patient-doctor interactions and preserving individuals' privacy. This entails a thorough analysis of mechanisms that delicately balance the ethical reuse of health data for research progress while respecting the sensitive nature of personal information on health.

Methodology

This report is based on a comprehensive research approach undertaken by the author, combining a literature review and direct engagement with experts in the field of healthcare digitisation and data. The primary research methodology involved in-person discussions, online meetings, and paper-based interviews with a total of eight experts representing diverse perspectives from the public sector, non-governmental organisations (NGOs) and academia.

The research started with an extensive literature analysis to establish a foundational understanding of the current discourse on healthcare digitalisation and data. This phase involved a thorough examination of academic articles, reports and relevant publications to identify key themes, challenges and potential solutions in the field.

In the expert selection phase, the author identified experts renowned in the fields of healthcare, digitalisation and data. These experts were strategically chosen to ensure a comprehensive representation of perspectives from the public sector, NGOs and academia, and from diverse backgrounds, with the aim of providing a holistic view of the challenges and opportunities in the field.

Further, in-person discussions, online meetings and paper-based interviews were conducted with the selected experts to gather insights and opinions. The interviews were based on predefined questions but allowed for open discussion. Given the sensitive nature of the topic, and to encourage open dialogue, the author ensured the confidentiality of some of the responses. Not all experts agreed to be quoted directly, and their anonymity was respected. Consequently, only a portion of the interviews is made public in the report, with the non-attributed insights contributing to the overall findings.

The collected data was analysed and the findings obtained from the literature review, were synthesised with the expert interviews to form the basis of the report. This multifaceted research methodology aims to provide a comprehensive and well-rounded exploration of the subject matter, offering valuable insights into the challenges and potential pathways for advancing secondary health data sharing in Poland.