



Data sovereignty requirements for patient-oriented AI-driven clinical research in Germany

Marija Radic · Julia Busch-Casler · Agnes Vosen · Philipp Herrmann · Arno Appenzeller · Henrik Mucha · Patrick Philipp · Kevin Frank · Stephanie Dauth · Michaela Köhm · Berna Orak · Indra Spiecker genannt Döhmann · Peter Böhm

Received: 19 January 2024 / Accepted: 15 May 2024
© The Author(s) 2024

Abstract

Background The rapidly growing quantity of health data presents researchers with ample opportunity for innovation. At the same time, exploitation of the value of Big Data poses various ethical challenges that must be addressed in order to fulfil the requirements of responsible research and innovation (Gerke et al. 2020; Howe III and Elenberg 2020). Data sovereignty and its principles of self-determination and informed consent are central goals in this endeavor. However, their consistent implementation has enormous consequences for the collection and processing of data

This article is published in the context of the special issue: “Ethik in der datenintensiven medizinischen Forschung”.

✉ Dr. Marija Radic · Dr. Julia Busch-Casler · Dr. Agnes Vosen · Philipp Herrmann, MSc
Fraunhofer Center for International Management and Knowledge Economy IMW,
Martin-Luther-Ring 13, 04109 Leipzig, Germany
E-Mail: marija.radic@imw.fraunhofer.de

Arno Appenzeller, MSc
Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany

Henrik Mucha · Patrick Philipp
Fraunhofer Institute for Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe, Germany

Dr. Kevin Frank · Stephanie Dauth, PhD · Dr. med. Michaela Köhm
Fraunhofer-Institute for Translational Medicine and Pharmacology ITMP, Frankfurt, Germany

Stephanie Dauth, PhD · Dr. med. Michaela Köhm
Fraunhofer Cluster of Excellence Immune-Mediated Diseases CIMD, Frankfurt, Germany

Berna Orak · Prof. Dr. Indra Spiecker genannt Döhmann, LL.M.
Chair of Public and Administrative Law, Information Law, Environmental Law and Legal Theory,
Goethe University Frankfurt, Frankfurt, Germany

Peter Böhm
Deutsche Rheuma-Liga e. V., Bonn, Germany

in practice, especially given the complexity and growth of data in healthcare, which implies that artificial intelligence (AI) will increasingly be applied in the field due to its potential to unlock relevant, but previously hidden, information from the growing number of data (Jiang et al. 2017). Consequently, there is a need for ethically sound guidelines to help determine how data sovereignty and informed consent can be implemented in clinical research.

Methods Using the method of a narrative literature review combined with a design thinking approach, this paper aims to contribute to the literature by answering the following research question: What are the practical requirements for the thorough implementation of data sovereignty and informed consent in healthcare?

Results We show that privacy-preserving technologies, human-centered usability and interaction design, explainable and trustworthy AI, user acceptance and trust, patient involvement, and effective legislation are key requirements for data sovereignty and self-determination in clinical research. We outline the implications for the development of IT solutions in the German healthcare system.

Keywords Data sovereignty · Informed consent · Artificial intelligence · German healthcare system · Big Data

Anforderungen an die Datensouveränität in der patientenorientierten und KI-gestützten klinischen Forschung in Deutschland

Zusammenfassung

Hintergrund Die exponentiell wachsende Verfügbarkeit von Gesundheitsdaten bietet Forschenden ungeahnte Potenziale für Innovationen. Gleichzeitig gehen mit der Verwertung von Big Data auch große ethische Herausforderungen einher, die es zu bewältigen gilt, um den Anforderungen an verantwortungsvolle Forschung und Innovation gerecht zu werden (Gerke et al. 2020; Howe III und Elenberg 2020). Datensouveränität und die damit verbundenen Grundsätze der Selbstbestimmung und der informierten Zustimmung sind dabei zentrale Ziele. Allerdings hat deren konsistente Umsetzung enorme Konsequenzen für die Datenerhebung und -verarbeitung in der Praxis. Dies trifft insbesondere angesichts einer Zunahme an Quantität und Komplexität von Daten im Gesundheitswesen zu. Denn aufgrund des Potenzials, relevante aber bisher verborgene Informationen aus der Datenmenge zu erschließen, ist eine zunehmende Anwendung von künstlicher Intelligenz (KI) in diesem Bereich zu erwarten (Jiang et al. 2017). Folglich besteht ein Bedarf an ethisch fundierten Handlungsanweisungen, die helfen, Datensouveränität und informierte Zustimmung in der klinischen Forschung umzusetzen.

Material und Methoden Durch Anwendung einer narrativen Literaturrecherche in Kombination mit einem Design-Thinking-Ansatz soll das vorliegende Papier einen Beitrag zur Literatur leisten, indem die folgende Forschungsfrage beantwortet wird: Welche praktischen Anforderungen gibt es für eine konsequente Umsetzung von Datensouveränität und informierter Einwilligung im Gesundheitswesen?

Ergebnisse Es wird gezeigt, dass Privatsphäre wahrende Technologien, menschenzentriert entwickelte Nutzungs- und Interaktionslösungen, erklärbare und vertrauens-

würdige KI, Nutzerakzeptanz und -vertrauen, Patientenbeteiligung und eine wirksame Gesetzgebung zentrale Voraussetzungen für Datensouveränität und Selbstbestimmung in der klinischen Forschung sind. Die Bedeutung für die Entwicklung von IT-Lösungen im deutschen Gesundheitssystem wird dargelegt.

Schlüsselwörter Datensouveränität · Informierte Zustimmung · Künstliche Intelligenz · Deutsches Gesundheitssystem · Big Data

Introduction

The re-use of health data for research, innovation, and policy-making offers great potential, which the European Commission (2022) is trying to capture by proposing the European Health Data Space (EHDS). While data are needed for any kind of (clinical) research, it is the use of large data sets, which could be made available by large-scale infrastructures such as the EHDS, that offers the opportunity to transform healthcare (Tretter et al. 2023). However, the application of artificial intelligence (AI) required to unlock the value of big data is fraught with ethical challenges (Howe III and Elenberg 2020; Gerke et al. 2020).

According to the German Ethics Council, “Data sovereignty [...] is the central ethical and legal goal in confronting the challenges and opportunities presented by big data” (German Ethics Council 2017, p. 30). Although not used uniformly throughout the literature, the concept of data sovereignty transfers the historical idea of a subject’s position of control within a domain to data processes, and at the same time it normatively demands that these should be able to articulate and assert corresponding claims (Hummel et al. 2018). This requires the implementation of technical measures to generate corresponding empowerment effects. From a regulatory standpoint, the concept of data sovereignty takes up important basic decisions already laid down in law and reinterprets them in a specific functionality (Hummel et al. 2021a). Self-determination and informed consent are central keys to the principle of patient data sovereignty. From the perspective of a data user that uses health data to generate value, the thorough implementation of data sovereignty measures can also be seen as a necessary condition to meet the requirements of responsible research and innovation as proposed in various European frameworks (European Commission 2011; Burget et al. 2017).

Although facets of data sovereignty have been widely discussed at a theoretical level in certain studies (e.g., Hummel et al. 2021a; Wiertz 2022), these studies do not take a stance on how to advance data sovereignty in clinical practice—especially when AI is involved. Considering the enormous implications for data collection and processing, there is a need for key pillars to guide the implementation of data sovereignty and informed consent in clinical research, ideally in a standardized way. This complex task requires an exploratory, multidisciplinary approach and perspectives from varying fields of research as well as patients (Hummel et al. 2018). Using the qualitative method of a narrative literature review in combination with a design thinking approach, we contribute to the discussion by answering the research question: What are the practical requirements for an AI-ready implementation of

data sovereignty and informed consent? The paper is structured as follows: The next section will outline the methodology of our study, followed by a presentation of the results. The study closes with a discussion of the findings and a conclusion.

Methodology

Answering our complex research question requires an exploratory and therefore qualitative, cross-disciplinary, and multidisciplinary approach involving several fields of science and learning. Sharing knowledge has generated a great interest in design thinking, which has been applied in many organizations and institutions in an attempt to acquire creative thinking and a broader vision—broader problem-solving for user-centered innovation (Inglesis Barcellos and Botura 2018). Design thinking can be described as a strategy to solve complex problems with the help of researchers from different disciplines (Wölbling et al. 2012). Various process models of design thinking exist. A common model from the HPI School of Design Thinking uses a systematic approach consisting of six phases: understand, observe, define the point of view, ideate, prototype, and test. The design thinking process is non-linear and iterative.

In line with Lauf et al. (2022), we modify this original design by transforming the stated phases to adapt the approach to our research purposes: awareness building, knowledge building, point of view, ideate, concept development, and validation. These adaptations were necessary because our approach is a conceptual research methodology rather than a more technical procedure commonly used in design thinking. Specifically, we applied literature reviews in the first two phases while changing phases five and six from a prototyping focus to concept developments and focus group discussions. The adapted iterative approach is shown in Fig. 1, with an embedded loop from the last to the first phase to support an agile research process.

Our research group consists of 15 members with backgrounds in different disciplines, including the authors and additional researchers. Starting with *awareness building*, the researchers developed their own understanding of the possible requirements for data sovereignty and informed consent and the consequential implications for the development of IT solutions in the German healthcare system. Subsequently, in the second phase of *knowledge building*, the researchers conducted a narrative literature analysis within their field of research to obtain comprehensive information on potential requirements. Compared with a systematic literature review, a narrative literature review is more flexible and reflective (Pautasso 2019) and therefore better suited to the iterative and agile nature of our design thinking process. After

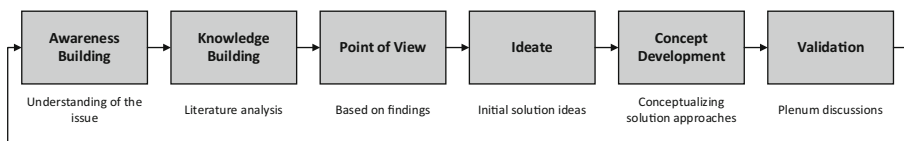


Fig. 1 Methodology based on a Design Thinking process with six phases (HPI School of Design Thinking 2022)

this step, each researcher formed an individual *point of view*, based on the insights accumulated from the previous phases. In the phase of *ideate*, the researchers relied on the rather subjective insights that they gained to generate different ideas. These initial ideas were transformed into concrete requirements and implications in the subsequent *concept development* phase.

While the researchers worked independently in the five phases described so far, the final phase of *validation* was carried out in focus groups. Focus groups are appropriate when the researcher wants to obtain a variety of possibly divergent perspectives on a selected topic in order to capture the issue at hand as holistically as possible (Stewart 2014). In addition to the 15 researchers, two patient representatives participated in order to validate the concepts from a patient perspective. The focus groups used recommended collaborative tools such as digital whiteboards and presentations to support the research process (Brown 2008). After the third iteration of plenum discussions, the research process ended as there was a high level of perceived congruence between all researchers and patient representatives.

Results

The following sections describe the central requirements for a practical implementation of data sovereignty and informed consent as a central goal to overcome the ethical challenges associated with the use of big data in health. As a result of our study, we identified six requirements that will be outlined in detail here. While only the third requirement explicitly deals with AI, all of the other requirements are also necessary conditions for its application (Table 1).

The concerns underlying the *first requirement* are supported by recent work on medical AI ethics (Tang et al. 2023). It aims to enable data sovereignty and informed consent through three fundamental technologies: a digital consent management system, privacy-preserving technologies, and privacy risk quantification. Informed consent for medical data is required by the European General Data Protection Regulation (GDPR) Art. 9(2), and thus digital consent management systems can facilitate this process. The GDPR outlines specific conditions for data processing, with explicit consent from the data subject being a common legal basis for medical research. As the volume of medical data increases, granular consent management becomes essential (Appenzeller et al. 2020) to facilitate active patient participation and engagement. Appenzeller et al. (2022) propose a workflow for

Table 1 Key requirements for practical implementation of data sovereignty and informed consent

Key requirements

1. Implement technologies to enable data sovereignty and informed consent
2. Apply usability and interaction design standards within the healthcare software
3. Implement state-of-the art knowledge to ensure trustworthy AI
4. Ensure fulfillment of several criteria related to user acceptance and trust
5. Ensure rigorous patient involvement, especially if data are being donated
6. Formulate effective legislation that balances different interests

sovereign dynamic consent that prioritizes patient involvement and provides a technical system for granular decisions with quantification of privacy impact, thereby enhancing informed consent decisions. Another fundamental part for patient-centered research is the use of privacy-preserving technologies. While anonymization and pseudonymization are commonly used methods in medical research, there is also a need for privacy-preserving technologies. To mitigate re-identification risks (Sweeney 2002), various privacy-preserving technologies exist (Dwork 2008) and have already been successfully implemented in a large-scale real-world use case (Kenny et al. 2021). The final technological building block we have identified for data sovereignty is the quantification of privacy risks. While digital consent empowers the patient, on the one hand, the degree of choice can potentially overwhelm the data subject, on the other hand (Appenzeller et al. 2022). Therefore, comprehensible privacy risk quantification should support patients in their decision to share data. Privacy risk quantification for personal data includes two main approaches: data-based quantification, which analyzes shared data for factors such as uniqueness and regulatory fines, and rule-based quantification, which examines privacy policies and text-based regulations that affect data privacy (Deußer et al. 2020; Kelley et al. 2009).

The *second requirement* aims to achieve data sovereignty and informed consent through the rigorous application of usability and interaction design standards in healthcare software. This requirement was identified because healthcare software currently suffers from poor usability and interface design (Wachter 2017). However, both aspects are essential to ensure that data sovereignty and informed consent can be achieved in practice by end users (Feth 2023). The principles of human-centered design and engineering are well understood and outlined. As such, there are three key documents that should be implemented in a software development process. Firstly, ISO 9241-210 (International Organization for Standardization 2019) provides the terminology needed to work towards usable software and describes the human-centered design process and its activities. Secondly, ISO 9241-110 (International Organization for Standardization 2020) provides guidelines on the fundamental qualities of usable software. To be considered usable, software must fulfil seven principles (suitability for user's task, self-descriptiveness, conformity with user expectations, learnability, controllability, user error robustness, user engagement) which are described in more detail in the document. Finally, DIN EN ISO 13485 (International Organization for Standardization 2022) specifies requirements for a quality management system in which an organization must demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements. The document describes the need for thorough documentation, particularly with regard to design documentation.

The *third requirement* concerns the implementation of state-of-the-art knowledge to ensure trustworthy AI. Although AI and machine learning approaches have the potential to significantly advance clinical research (Yu et al. 2018), their application must be developed to meet specific quality standards and be secured against their risks (Beck et al. 2023; Gerke et al. 2020). The concept of trustworthy AI has been identified to be central for achieving this. The concept has three main components: “(1) it should comply with the law, (2) it should fulfil ethical principles and (3) it

should be robust” (European Commission 2019, p. 3). Based on these key parameters and the EU core values, the EU identified seven key requirements for trustworthy AI: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) societal and environmental well-being, and (7) accountability (European Commission 2019). Putting these rather abstract requirements into practice is still a challenge, as their implementation is highly dependent on the type of technology used and the field of application. One way to define application-specific quality criteria is a risk-based approach (Poretschkin et al. 2021). In this approach, the object to be analyzed is specified and evaluated along six dimensions of trustworthiness (fairness, autonomy and control, transparency, reliability, safety and security, data protection). The risk-based approach has already been proven in classic IT security and functional safety (Aleksandrov et al. 2021) and can therefore serve as a means to assess and optimize the trustworthiness of AI for healthcare software. However, Botsman (2017) and Tretter et al. (2023) point out that it will continue to be the central task of human personnel to act as trust-bearers in clinical contexts and to ensure that this trust is constantly maintained.

As a *fourth requirement*, a health information exchange platform must also meet several criteria related to user acceptance and trust, as existing research has shown that while patients recognize the potential for secondary use of health data, concerns about trust, privacy, and transparency are widespread (Hutchings et al. 2020). By iterating existing knowledge in the literature with the patient representatives involved in the research group, we identified three factors as being most critical for patient acceptance: the safety and soundness of the application; the transparency of the application’s data use and privacy policies; and the convenience, ease of access, and immediate availability of the application. Safety and soundness of the application refers to the expectation and perception that the technology will carry out certain processes according to the user’s wishes and assumptions, while not harming the user in any way (Backhaus 2017; Hutchings et al. 2020). There are certain specificities related to digital trust, mainly because there is no direct interaction with another physical party (Taddeo 2009). However, research on trust transfer theory shows that patients tend to transfer their initial cognitive trust in their healthcare provider to the health IT application (Lu et al. 2011; McKnight et al. 2002). This highlights the importance of involving key healthcare users in the development and deployment of applications. To increase trust, developers should also implement trust-building measures such as informational accuracy, understandability, and the promotion of autonomy and patient empowerment, as recommended by van Haasteren et al. (2020). Second, the transparency of the application’s data use and privacy policies relate particularly to what types of data are shared for what purpose and with whom, the duration of data storage, and the security measures taken to ensure data privacy (Hutchings et al. 2020; Mangal et al. 2022). Finally, the convenience, ease of access, and immediate availability of the application are important, which are relevant for both the patient and the healthcare provider (Hassol et al. 2004; Vergouw et al. 2020).

As a *fifth requirement*, in a scenario where individuals donate their data for secondary use, rigorous patient involvement should be ensured (Saelaert et al. 2023).

In order to comply with legal requirements and to enable informed decision-making, patients are required to provide their consent when participating in a medical research study, which is usually a very narrow consent to use data for a specific purpose for a predefined period of time. This obviously limits the use of the data for that purpose and does not allow for secondary analyses or inclusion in other potentially relevant medical research. The term “data donation” has been coined in Germany to expand the use of data in medical research (Molnár-Gábor 2021). It is the approval of using personal health information for medical research given at a specific point in time after detailed explanation of the consequences (Bundesministerium für Gesundheit 2020). Patients donate their data for research without receiving any compensation and justify their decision mainly with altruism, solidarity, gratitude, and generally supporting a common good (Richter et al. 2018). Self-determination in the context of data donation requires understandable and comprehensive information about the goals, processes, and specific projects of secondary use. These criteria also apply when AI is used to process the data (Perni et al. 2023). All data donation scenarios require high-quality citizen participation and the promotion of social data literacy as accompanying measures. The realization of self-determination through an opt-in broad consent faces significant practical and ethical challenges. Against this background, the ethical benefits of a quality-assured opt-out scenario are currently being discussed (Strech et al. 2020).

The *sixth requirement* is to develop effective legislation that balances different interests in order to achieve data sovereignty (Hummel et al. 2021b). In general, the processing of health data is allowed if there is consent or if there is Union or Member State law that provides for the processing. The GDPR sets out specific rules for the processing of sensitive data such as health data. The processing of this type of data is prohibited. Only with certain exceptions can the categories of data listed in Art. 9 (1) GDPR be processed. The regulation therefore contains opening clauses that allow for national implementation; cf. Art. 9 (2) GDPR (Kuner et al. 2020). Typically, data are not processed primarily for research purposes, but for the individual diagnosis and treatment of an individual patient. Research purposes therefore constitute a so-called secondary use. This secondary use of data causes great difficulties in practice regarding their legitimate use and the extent of such use, due to the vagueness of the underlying provisions (Peloquin et al. 2020). The GDPR grants privileges for the secondary use of data sets for research purposes; see Art. 5 (1)(b) GDPR. At the same time, the regulation strengthens the sovereignty of individuals by granting certain rights (see Art. 13 GDPR). Whenever health data are processed and Art. 9(2) GDPR is the legal basis, the safeguards of Art. 89 GDPR must be respected (Kuner et al. 2020).

By contrast, the current national legislation is more research-friendly. In the past 3 years, the German parliament has passed two new laws to expand digitization in the healthcare system. In November 2019, the Digital Healthcare Act (DVG) was passed with the aim of promoting digitization in the healthcare sector. A central database is planned in which the health data of around 90% of the German population will be stored (Schrahe and Städter 2020). Later, these data will also be made available to third parties for research purposes. Additionally, in October 2020, the Patient Data Protection Act (PDSG) came into force. From 2023 on, insured persons will have

the option of voluntarily making some of their health data stored in their electronic health record available for research (Bretthauer and Spiecker genannt Döhmann 2020; Orak 2021). Both laws, in combination with the GDPR and other national laws based on the opening clauses thereof, have a major impact on the research of health data in combination with AI (Bretthauer and Spiecker genannt Döhmann 2020; Weichert 2020a; see BVerfG decision of the Second Chamber of the First Senate of 19 March 2020, No. 1 BvQ 1/20-, Rn. 1–18).

Furthermore, the use of vague terms in the GDPR leaves unanswered the scope of the privilege for scientific research. There is no legally binding definition of the term “scientific research” at the European level, which could lead to different interpretations and consequently raise various questions (Forgo 2015; Roßnagel 2019). The GDPR attempts to strike a balance between the two conflicting fundamental rights—the freedom of research and the right to data protection. In the context of research data processing, the freedom of research according to Art. 13 EU Charter of Fundamental Rights (CFR) and the protection of personal data according to Art. 8 CFR—are in conflict. According to Art. 13 CFR, research is an activity aimed at acquiring new knowledge in a methodical, systematic, and verifiable manner (Jarass 2021). Applied research is covered, but not the mere application of previously acquired knowledge. It is irrelevant whether the findings are scientifically recognized and where the research takes place. The regulatory content of Art. 13 CFR largely corresponds to that of Art. 5 (3) *Grundgesetz* and is inspired by it (Weichert 2020b). All in all, scientific research is understood in a broad sense. This is also confirmed by Recital 159 GDPR. Although Art. 13 CFR does not limit the scope of protection, it must be limited in the event of conflicting fundamental rights: see Art. 52 (1) CFR. Otherwise, freedom of research would mean that data protection would pale into insignificance (Spiecker genannt Döhmann 2021). The fact that both fundamental rights have to be balanced is also shown by Art. 89 GDPR (Spiecker genannt Döhmann 2021). It strengthens the protection of personal data. Art. 89 (2) and (3) GDPR, however, provide for exceptions to the rights of the data subject, which protects the freedom of research (Kuner et al. 2020).

From a legal perspective, the first step is therefore to formulate effective legislation. The secondary use of health data does not only allow for the processing of the collected data for other purposes, but also limits the rights of data subjects. It is important not only to conduct research, but also to regulate it in a way that respects fundamental rights, and this has become increasingly important in the context of the GDPR.

Discussion

By applying a narrative literature review combined with a design thinking approach, we were able to derive six requirements that need to be met to implement data sovereignty and informed consent in AI-enabled clinical research. Based on the existing literature, the requirements were operationalized into concrete implications for the development of ethical IT solutions. These are summarized in Table 2.

Table 2 Implications for IT solution development preserving patient data sovereignty and informed consent within the German healthcare system

Requirement	Implications
Implement technologies to enable data sovereignty and informed consent	Implement digital consent management system Implement privacy-preserving technologies Introduce privacy risk quantification automated consent management
Apply usability and interaction design standards within the healthcare software	Use human-centered design process Adhere to applicable standards to ensure state-of-the-art design and engineering
Implement state-of-the art knowledge to ensure trustworthy AI	Precisely specify use case of AI and map against criteria for trustworthy AI Consider implementation of risk-based approaches to evaluate AI trustworthiness
Ensure fulfillment of several criteria related to user acceptance and trust	Ensure safety and soundness of the application Implement trust-building measures in the development of the application (e.g., transparency, usability, privacy measures) Create transparency of data usage/privacy policies Ensure ease of access and availability of application
Ensure rigorous patient involvement, especially if data are being donated	Ensure high-quality citizen participation Promote data literacy Consider ethical challenges when realizing data sharing as an opt-out scenario
Formulate effective legislation that balances different interests	Provide clearly defined context to increase willingness of data sharing Create and communicate clear rules on secondary data use (research vs. commercial use) Balance data protection vs. scientific freedom

Our study advances existing knowledge from both a theoretical and a practical perspective. From a theoretical perspective, other authors have examined how data sovereignty can be achieved in a data-sharing use case primarily from an ethical perspective. In particular, Hummel et al. (2018) propose to adopt data sovereignty and informed consent as normative reference points for responsible and ethically sound data-sharing mechanisms. Their recommendations overlap with our requirements. For example, Hummel et al. (2018) highlight the responsibility of multiple stakeholders and levels to achieve data sovereignty. They also emphasize that individuals have a right to education on data literacy, while at the same time technology should be designed to be easy to understand so as not to overwhelm individuals with information they cannot process. On the other hand, it is clear that the recommendations presented are not specifically tailored to the healthcare use case, as several of them aim to balance individual claims for data sovereignty against market dynamics (e.g., by ensuring data interoperability or a plurality of data platforms). However, the case for healthcare is different, as the likely evolution in Europe is towards a much more regulated value chain with few actors. Furthermore, the recommendations put forward are very theoretical in nature. Therefore, we believe that our paper adds value by targeting the recommendations to a healthcare use case, taking into ac-

count the latest legislative initiatives at both EU and national level such as, e.g., the EHDS (European Commission 2022), the AI Act (European Commission 2021), or the Health Data Utilization Act (Bundesministerium für Gesundheit 2023; see also Ebert and Spiecker gen. Döhmman 2021; Kühling and Schildbach 2024; Roos and Maddaloni 2023). In addition, our requirements are underpinned by implications that pave the way for implementation.

From a practical perspective, the German Ethics Council (2017) has put forward recommendations to implement data sovereignty as a guiding principle for the use of big data in health. The recommendations aim at realizing the potential of big data, preserving individual freedom and privacy, ensuring fairness and solidarity, and promoting responsibility and trust. Again, there is an overlap with the requirements derived from our research. However, the paper falls short in providing evidence-based tools and measures to guide implementation. Furthermore, both the technical and legal frameworks have evolved significantly since the publication of the paper. In summary, our study contributes to the literature by providing up-to-date and evidence-based practical guidelines on how to implement data sovereignty and informed consent in a healthcare setting.

Conclusion

Achieving patient-centered AI-driven clinical research requires data sovereignty and informed patient consent. The complexity of the context requires a cross-disciplinary approach and active patient involvement in the development of solutions. We identify six requirements, which are further substantiated with concrete implications for the development of IT solutions in the German healthcare system. The paper thus closes a research gap by providing key pillars on how data sovereignty in clinical research can be implemented in practice. We recommend three directions for further research in the field.

First, we have identified several approaches, tools, and standards that are suitable for achieving data sovereignty and informed consent in a healthcare context. However, most of these approaches have not yet been sufficiently implemented. For example, although standards for usability and interaction design standards are well documented, existing healthcare technologies still perform poorly in this regard. Similarly, risk-based approaches to assess AI trustworthiness have proven valuable, but not yet in the context of clinical research.

Secondly, we have outlined in detail the legal challenges of secondary data use that are rooted in the current legislation. Further efforts are needed to balance the interests of all stakeholders (patients, clinical researchers, national governments, etc.) in order to develop a legal framework that adequately addresses the different legitimate needs while enabling innovation through data use.

Thirdly, in our study we took great care to include different scientific perspectives as well as patient representatives. Collaboration between many disciplines and end users is needed to digitally enable data sovereignty and informed consent. It is this collaboration between different disciplines itself, and the involvement of patient research partners to represent the patient perspective, that has made the analysis

of requirements presented here possible and offers much potential for scientific progress. Our results point to the need for extensive stakeholder involvement in the development of the architecture of future IT solutions for the secondary use of healthcare data. Contributions on stakeholder involvement have been made both in healthcare and in other fields (Hendricks et al. 2018; Reed 2008). We therefore call on researchers to develop a stakeholder participation agenda to support the development of the EU-wide health data sharing solution. In addition to drawing on existing research, such an agenda should also incorporate learning from countries that have already implemented such a solution.

Acknowledgements We would like to thank all members of the DATACARE research team for their contributions during the workshops and the preparations of this paper.

Funding The underlying research project was funded by the German Federal Ministry of Education and Research with the funding number 01GP2112A—DATACARE—Data sovereignty and informed consent as enablers for patient-oriented AI-driven clinical research. The responsibility for the content of this paper lies with the authors.

Author Contribution All authors researched the literature and participated in writing the first draft of the manuscript. All authors reviewed and edited the manuscript and approved the final version of the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of interest M. Radic, J. Busch-Casler, A. Vosen, P. Herrmann, A. Appenzeller, H. Mucha, P. Philipp, K. Frank, S. Dauth, M. Köhm, B. Orak, I. Spiecker genannt Döhm and P. Böhm declare that they have no competing interests.

Ethical standards For this article no studies with human participants or animals were performed by any of the authors. All studies mentioned were in accordance with the ethical standards indicated in each case.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Aleksandrov MN, Vasiliev VA, Aleksandrova SV (2021) Implementation of the risk-based approach methodology in information security management systems. In: 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp 137–139
- Appenzeller A, Rode E, Krempel E, Beyerer J (2020) Enabling data sovereignty for patients through digital consent enforcement. Proceedings of the 13th ACM International Conference on Pervasive Technologies Related to Assistive Environments, pp 1–4

- Appenzeller A, Hornung M, Kadow T, Krempel E, Beyerer J (2022) Sovereign digital consent through privacy impact quantification and dynamic consent. *Technologies* 10(1):35. <https://doi.org/10.3390/technologies10010035>
- Backhaus N (2017) Nutzervertrauen und -erleben im Kontext technischer Systeme. Technische Universität Berlin, Berlin (Doctoral dissertation)
- Beck S, Faber M, Gerndt S (2023) Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege. *Ethik Med* 35(2):247–263. <https://doi.org/10.1007/s00481-023-00763-9>
- Botsman R (2017) Who can you trust? How technology brought us together—and why it could drive us apart. Portfolio Penguin, London
- Brethauer S, Spiecker genannt Döhmhann I (2020) Das Digitale-Versorgung-Gesetz als Einfallstor für eine Neujustierung von einstweiligem Rechtsschutz vor dem BVerfG und der Eingriffsqualität bei Datenverwendungen. *JuristenZeitung* 75(20):990–996. <https://doi.org/10.1628/jz-2020-0326>
- Brown T (2008) Design thinking. *Harv Bus Rev* 86(6):84–92
- Bundesministerium für Gesundheit (2020) „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf. Accessed 8 Nov 2023
- Bundesministerium für Gesundheit (2023) Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/G/GDNG_Kabinett.pdf. Accessed 24 May 2024
- Burget M, Bardone E, Pedaste M (2017) Definitions and conceptual dimensions of responsible research and innovation: a literature review. *Sci Eng Ethics* 23(1):1–19. <https://doi.org/10.1007/s11948-016-9782-1>
- Deußer C, Passmann S, Strufe T (2020) Browsing unicity: on the limits of anonymizing web tracking data. 2020 IEEE Symposium on Security and Privacy, pp 777–790 <https://doi.org/10.1109/SP40000.2020.00018>
- Dwork C (2008) Differential privacy. International conference on theory and applications of models of computation, pp 1–12
- Ebert A, Spiecker genannt Döhmhann I (2021) Der Kommissionsentwurf für eine KI-Verordnung der EU. *Neue Z Verwaltungsr* 16:1161–1240
- European Commission (2011) Proposal for a regulation of the European Parliament and of the Council establishing Horizon 2020—The Framework Programme for Research and Innovation (2014–2020). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011PC0809>. Accessed 23 May 2024
- European Commission (2019) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building trust in human-centric artificial intelligence. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58496. Accessed 23 Nov 2023
- European Commission (2021) Proposal for a regulation of the European Parliament and of the Council. Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>. Accessed 24 May 2024
- European Commission (2022) Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space. Report No.: COM/2022/197 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>. Accessed 28 Mar 2024
- Feth D (2023) Usable Implementation of data sovereignty in digital ecosystems. International Conference on Human-Computer Interaction, pp 135–150 https://doi.org/10.1007/978-3-031-35822-7_10
- Forgo N (2015) My health data—your research: some preliminary thoughts on different values in the General Data Protection Regulation. *Int Data Priv Law* 5(1):54–63. <https://doi.org/10.1093/idpl/ipu028>
- Gerke S, Minssen T, Cohen G (2020) Chapter 12—Ethical and legal challenges of artificial intelligence-driven healthcare. In: Bohr A, Memarzadeh K (eds) *Artificial intelligence in healthcare*. Academic Press, London, San Diego, CA, Cambridge, pp 295–336
- German Ethics Council (2017) Big data and health—Data sovereignty as the shaping of informational freedom [executive summary & recommendations]. <https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf>. Accessed 29 Nov 2023
- van Haasteren A, Vayena E, Powell J (2020) The mobile health app trustworthiness checklist: usability assessment. *JMIR Mhealth Uhealth* 8(7):e16844. <https://doi.org/10.2196/16844>

- Hassol A, Walker JM, Kidder D, Rokita K, Young D, Pierdon S, Deitz D, Kuck S, Ortiz E (2004) Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *J Am Med Informatics Assoc* 11(6):505–513. <https://doi.org/10.1197/jamia.M1593>
- Hendricks S, Conrad N, Douglas TS, Mutsvangwa T (2018) A modified stakeholder participation assessment framework for design thinking in health innovation. *Healthcare* 6(3):191–196. <https://doi.org/10.1016/j.hjdsi.2018.06.003>
- Howe EG III, Elenberg F (2020) Ethical challenges posed by big data. *Innov Clin Neurosci* 17(10–12): 24–30
- HPI School of Design Thinking (2022) The six phases of the design thinking process. <https://hpi.de/en/school-of-design-thinking/design-thinking/background/design-thinking-process.html#%3A%7E%3Atext%3D%2520The%2520six%2520phases%2520of%2520the%2520Design%2520Thinking%2Cideas%2520up%2520to%2520a%2520necessary%2520level%2%80%A6%2520More%2520> Accessed 23 Nov 2023
- Hummel P, Braun M, Augsberg S, Dabrock P (2018) Sovereignty and data sharing. *ITU J ICT Discov* 1(2)
- Hummel P, Braun M, Dabrock P (2021a) Own data? Ethical reflections on data ownership. *Philos Technol* 34(3):545–572. <https://doi.org/10.1007/s13347-020-00404-9>
- Hummel P, Braun M, Tretter M, Dabrock P (2021b) Data sovereignty: a review. *Big Data Soc* 8(1):1–17. <https://doi.org/10.1177/2053951720982012>
- Hutchings E, Loomes M, Butow P, Boyle FM (2020) A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on privacy, trust, and transparency. *Syst Rev* 9(1):235. <https://doi.org/10.1186/s13643-020-01481-9>
- Inglis Barcellos EE, Botura G (2018) Design thinking: User-centered multidisciplinary methodology based on people and innovation. In: Kantola J, Barath T, Nazir S (eds) *Advances in human factors, business management and leadership Proceedings of the AHFE 2017 International Conferences on Human Factors in Management and Leadership, and Business Management and Society, The Westin Bonaventure Hotel, Los Angeles., July 17–21, 2017. vol 8. Springer*, pp 173–182 https://doi.org/10.1007/978-3-319-60372-8_17
- International Organization for Standardization (2019) ISO 9241-210:2019 Ergonomics of human-system interaction: Part 210: Human-centred design for interactive systems. <https://www.iso.org/standard/77520.html>. Accessed 23 Nov 2023
- International Organization for Standardization (2020) ISO 9241-110 Ergonomics of human-system interaction: Part 110: Interaction principles. <https://www.iso.org/standard/38009.html#:~:text=ISO%209241%2D110%3A2006%20focuses,dialo%20principles%20is%20not%20exhaustive>. Accessed 23 Nov 2023
- International Organization for Standardization (2022) ISO 13485 Medical devices. <https://www.iso.org/iso-13485-medical-devices.html>. Accessed 23 Nov 2023
- Jarass HD (2021) *Charta der Grundrechte der Europäischen Union: Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK: Kommentar*, 4th edn. C.H. Beck, München
- Jiang F, Jiang Y, Zhi H, Dong Y, Li H, Ma S, Wang Y, Dong Q, Shen H, Wang Y (2017) Artificial intelligence in healthcare: past, present and future. *Stroke Vasc Neurol* 2(4):230
- Kelley PG, Bresee J, Cranor LF, Reeder RW (2009) A “nutrition label” for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security*, pp 1–12 <https://doi.org/10.1145/1572532.1572538>
- Kenny CT, Kuriwaki S, McCartan C, Rosenman ETR, Simko T, Imai K (2021) The use of differential privacy for census data and its impact on redistricting: The case of the 2020 U.S. Census. *Sci Adv* 7(41):eabk3283. <https://doi.org/10.1126/sciadv.abk3283>
- Kühling J, Schildbach R (2024) Datenschutzrechtliche Spielräume für eine forschungsfreundliche digitale Gesundheitsversorgung – von DSGVO, SGB etc. zur EHDS-VO und zum GDNG. *Z Digit Recht* (1):1–26
- Kuner C, Bygrave LA, Docksey C, Drechsler L, Alvarez Rigaudias C (eds) (2020) *The EU general data protection regulation (GDPR): a commentary*, 1st edn. Oxford University Press, Oxford
- Lauf F, Scheider S, Bartsch J, Herrmann P, Radic M, Rebbert M, Nemat (2022) Linking data sovereignty and data economy: arising areas of tension. *Wirtschaftsinformatik 2022 Proceedings* 19. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19. Accessed 16 June 2024
- Lu Y, Yang S, Chau PY, Cao Y (2011) Dynamics between the trust transfer process and intention to use mobile payment services: a cross-environment perspective. *Inf Manag* 48(8):393–403. <https://doi.org/10.1016/j.im.2011.09.006>
- Mangal S, Park L, Reading Turchioe M, Choi J, de Rivera NS, Myers A, Goyal P, Dugdale L, Master-son Creber R (2022) Building trust in research through information and intent transparency with

- health information: representative cross-sectional survey of 502 US adults. *J Am Med Inform Assoc* 29(9):1535–1545. <https://doi.org/10.1093/jamia/ocac084>
- McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Inf Syst Res* 13(3):334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Molnár-Gábor F (2021) Ausgestaltung der Einwilligung in die Datenspende für die Gesundheitsforschung. *Datenschutz Datensicher* 45(12):799–805. <https://doi.org/10.1007/s11623-021-1540-0>
- Orak B (2021) Digitalization in Germany's health care system. In: SECURITY HORIZONS (ed) 30 Years Of Independent Macedonian State, vol 2, pp 131–138
- Pautasso M (2019) The structure and conduct of a narrative literature review. In: Shoja M, Arynchyna A, Loukas M, D'Antoni AV, Buerger SM, Karl M, Tubbs RS (eds) *A guide to the scientific career: virtues, communication, research and academic writing*. Wiley, pp 299–310 <https://doi.org/10.1002/9781118907283.ch31>
- Peloquin D, DiMaio M, Bierer B, Barnes M (2020) Disruptive and avoidable: GDPR challenges to secondary research uses of data. *Eur J Hum Genet* 28(6):697–705
- Perni S, Lehmann LS, Bitterman DS (2023) Patients should be informed when AI systems are used in clinical trials. *Nat Med* 29(8):1890–1891. <https://doi.org/10.1038/s41591-023-02367-8>
- Poretschkin M, Schmitz A, Akila M, Adilova L, Becker D, Cremers AB, Hecker D, Houben S, Mock M, Rosenzweig J, Sicking J, Schulz E, Voss A, Wrobel S (2021) Leitfaden zur Gestaltung vertrauenswürdiger Künstlicher Intelligenz: KI-Prüfkatalog. https://www.iais.fraunhofer.de/content/dam/iais/fb/Kuenstliche_intelligenz/ki-pruefkatalog/202107_KI-Pruefkatalog.pdf. Accessed 23 Nov 2023
- Reed MS (2008) Stakeholder participation for environmental management: A literature review. *Biol Conserv* 141(10):2417–2431. <https://doi.org/10.1016/j.biocon.2008.07.014>
- Richter G, Krawczak M, Lieb W, Wolff L, Schreiber S, Buyx A (2018) Broad consent for health care-embedded biobanking: understanding and reasons to donate in a large patient sample. *Genet Med* 20(1):76–82. <https://doi.org/10.1038/gim.2017.82>
- Roos P, Maddaloni J-M (2023) Regulierter Datenaustausch zur Gesundheitsforschung: Die legislativen Vorhaben für einen Europäischen Gesundheitsdatenraum und ein Gesundheitsdatennutzungsgesetz. *Recht Digit* 3:225–232
- Roßnagel A (2019) Datenschutz in der Forschung: Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen. *Z Datenschutz* 4:157–164
- Saelaert N, Mathieu L, van Hoof W, Devleeschauwer 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. *Arch Public Health* 81(1):168. <https://doi.org/10.1186/s13690-023-01182-4>
- Schrahe D, Städter T (2020) Gesundheits-Apps auf Rezept und Forschung mit Gesundheitsdaten. *Datenschutz Datensicher* 44(11):713–718. <https://doi.org/10.1007/s11623-020-1355-4>
- Spiecker genannt Döhmann I (2021) Die Regulierungsperspektive von KI/BigData in der Wissenschaft. In: Gethmann CF, Buxmann P, Distelrath J, Humm BG, Lingner S, Nitsch V, Schmidt JC, Spiecker genannt Döhmann I (eds) *Künstliche Intelligenz in der Forschung: Neue Möglichkeiten und Herausforderungen für die Wissenschaft*. Springer, pp 147–172 https://doi.org/10.1007/978-3-662-63449-3_6
- Stewart DW (2014) *Focus groups: theory and practice*, 3rd edn. Supplementary textbook. SAGE, Washington, D.C.
- Strech D, Graf von Kielmansegg S, Zenker S, Krawczak M, Semler SC (2020) BMG-Gutachten: „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen (TMF, 2019). https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf. Accessed 30 Nov 2023
- Sweeney L (2002) k-anonymity: A model for protecting privacy. *Int J Uncertain Fuzziness Knowledge Based Syst* 10(05):557–570. <https://doi.org/10.1142/S0218488502001648>
- Taddeo M (2009) Defining trust and e-trust. *Int J Technol Hum Interact* 5(2):23–35. <https://doi.org/10.4018/jthi.2009040102>
- Tang L, Li J, Fantus S (2023) Medical artificial intelligence ethics: a systematic review of empirical studies. *Digit Health*. <https://doi.org/10.1177/20552076231186064>
- Tretter M, Samhammer D, Dabrock P (2023) Künstliche Intelligenz in der Medizin: Von Entlastungen und neuen Anforderungen im ärztlichen Handeln. *Ethik Med* 36:7–29. <https://doi.org/10.1007/s00481-023-00789-z>

- Vergouw JW, Smits-Pelser H, Kars MC, van Houwelingen T, van Os-Medendorp H, Kort H, Bleijenberg N (2020) Needs, barriers and facilitators of older adults towards eHealth in general practice: a qualitative study. *Prim Health Care Res Dev* 21:e54. <https://doi.org/10.1017/S1463423620000547>
- Wachter RM (2017) *The digital doctor: Hope, hype, and harm at the dawn of medicine's computer age.* Business classics. McGraw-Hill, New York
- Weichert T (2020a) „Datentransparenz“ und Datenschutz. *MedR* 38(7):539–546. <https://doi.org/10.1007/s00350-020-5585-0>
- Weichert T (2020b) Die Forschungsprivilegierung nach der DSGVO. In: Hentschel A, Hornung G, Jandt S (eds) *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft.* Festschrift für Alexander Roßnagel zum 70. Geburtstag, 1st edn. Nomos, Baden-Baden, pp 419–436
- Wiertz S (2022) Die zeitliche Dimension des Broad Consent. *Ethik Med* 34(4):645–667. <https://doi.org/10.1007/s00481-022-00715-9>
- Wölbling A, Krämer K, Buss CN, Dribbisch K, LoBue P, Taherivand A (2012) Design thinking: an innovative concept for developing user-centered software. In: Maedche A, Botzenhardt A, Neer L (eds) *Software for people: fundamentals, trends and best practices.* Springer, Berlin Heidelberg, pp 121–136 https://doi.org/10.1007/978-3-642-31371-4_7
- Yu K-H, Beam AL, Kohane IS (2018) Artificial intelligence in healthcare. *Nat Biomed Eng* 2(10):719–731. <https://doi.org/10.1038/s41551-018-0305-z>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.