






# Sovereignly Donating Medical Data as a Patient: A Technical Approach

Florian Lauf<sup>1</sup><sup>a</sup>, Hendrik Meyer zum Felde<sup>2</sup><sup>b</sup>, Marcel Klötgen<sup>1</sup><sup>c</sup>, Robin Brandstädter<sup>3</sup><sup>d</sup>  
and Robin Schönborn<sup>1</sup><sup>e</sup>

<sup>1</sup>Fraunhofer Institute for Software and Systems Engineering ISST, Dortmund, Germany

<sup>2</sup>Fraunhofer Institute for Applied and Integrated Security AISEC, Garching near Munich, Germany

<sup>3</sup>Fraunhofer Institute for Experimental Software Engineering IESE, Kaiserslautern, Germany

**Keywords:** Medical Data Donation, Data Sovereignty, Patient Empowerment, Usage Control, International Data Spaces.


**Abstract:** Data is the new asset of the 21<sup>st</sup> century, and many new business models are based on data. However, data is also needed in the medical research domain, such as in the procedure of applying new machine learning methods for gaining new medical findings. Furthermore, the hurdle arises that medical data comprises personal data, and thus, it requires particular care and protection. Hence, patients must consent to the data donation process for general medical research but without selecting specific research projects. We argue that patients must gain more influence in the data donation process to cover this lack of data sovereignty. Therefore, we developed a concept and implementation empowering patients to make sovereign decisions about donating their medical data to specific medical research projects. Our work comprises concepts of the Medical Informatics Initiative, International Data Spaces, and MY DATA Control Technologies with new specific elements combining these components. This approach of patient empowerment enables a new kind of data sovereignty in the medical research domain.


## 1 INTRODUCTION


When considering the restriction of data usage and access by an individual or company, then we enter the scientific field of data sovereignty. Being sovereign as an individual means being able to determine which entities have access to one's own data and how this data may be processed. Furthermore, the current regulation in Europe dictates that individuals must be informed about storing and processing their personal data (European Parliament and Council of European Union, 2016). Additionally, individuals must explicitly give consent to each specific usage of their medical data. However, donating medical data for cutting-edge research is essential. For instance, the exploration of large amounts of data with machine learning methods results in some completely new


research approaches (Specht-Riemenschneider & Radbruch, 2021), but legal consent represents a challenge (Ohmann et al., 2017).


The Medical Informatics Initiative provides a first text-based template for patient consent forms (Medical Informatics Initiative, 2020) that is based on broad consent concepts (Bild et al., 2020; Caulfield & Kaye, 2009; Sheehan, 2011), especially for medical research, which serves as a step to simplify the process of donating medical data. Therefore, patients who want to donate their medical data to the medical research can consent into these forms. Both medical researchers and patients obtain clarity on how personal medical data is permitted to be used for further research due to the expressed information of the consent forms. In this paper, we extend the broad consent model and give patients additional freedom

<sup>a</sup> <https://orcid.org/0000-0003-0844-3722>

<sup>b</sup> <https://orcid.org/0000-0002-5837-8730>

<sup>c</sup> <https://orcid.org/0000-0003-4109-8641>

<sup>d</sup> <https://orcid.org/0000-0001-8439-3697>

<sup>e</sup> <https://orcid.org/0000-0001-7510-622X>

in decision-making. We present a mechanism that allows patients to decide individually for which research projects their medical data will be donated.

Furthermore, to ensure that an individual's choice of whether data transfer is permitted or prohibited, we enforce data use and access policies in a technical manner using International Data Spaces technology (IDSA, 2019). Using specific connectors, the related architecture dictates the conditions of securely transferring data for use and access. Thus, our research objective comprises a linking of separated concepts to design a trustworthy donation system for medical data and individual data sovereignty. We contribute to foster the involvement of patients in data donating processes and propose a technical system to realize this patient's empowerment. Consequently, we define the following research questions (RQ):

**RQ1:** How can patients be technically empowered to donate their medical data sovereignly to selected medical research projects?

**RQ2:** What are important components for an adequate implementation of such a concept?

The paper is structured as follows. In Section 2, we discuss related works that we have included in our conceptual approach. Data sovereignty of citizens, work of the Medical Informatics Initiative including the SMITH Service Platform, and International Data Spaces technology with embedded usage control are the pillars of our research. We integrated these previous works into our approach for donating medical data. Hence, we describe our concept in Section 3. Subsequently, the appropriate implementation is presented in Section 4. Afterward, in Section 5, we discuss our implemented concept. Finally, we outline our research in Section 6 and point out further research to create a comprehensive tool for patients to donate their own medical data.

## 2 RELATED WORK

This section describes the works related to our research into sovereign donation of medical data.

### 2.1 Data Sovereignty of Citizens

We understand data sovereignty as a subdomain of digital sovereignty that puts the asset 'data' in the spotlight (Adonis, 2019; Couture & Toupin, 2019; Otto, 2016). Furthermore, we state that data sovereignty of citizens is a means to comply with the informational self-determination required by the German legislator because the relevant data constitute

personal data (European Parliament and Council of European Union, 2016; Steinmüller et al., 1972). In addition, personal data comprises data that is created by and about an individual (World Economic Forum, 2011). Overall, we interpret the term data sovereignty as the knowledge and control of who can access an individuals' data and where this data is transferred (Posch, 2017).

However, insights into the data sovereignty of citizens show the lack of current solutions to share one's data in a self-determined way due to the inadequate abilities of citizens to make sovereign data-sharing decisions. However, the Digital Life Journey describes the digitized lives of citizens and addresses several areas being included in a holistic approach of citizens' data sovereignty (Meister & Otto, 2019). Initial use cases such as the project DaWID demonstrate how citizens can sovereignly participate in data ecosystems with their own personal data (Lauf et al., 2021).

### 2.2 Medical Informatics Initiative and SMITH Service Platform

The Medical Informatics Initiative (MII) aims at optimizing healthcare through providing interoperable primary care data for clinical and medical research (Semler et al., 2018), according to the FAIR data principles (Wilkinson et al., 2016). Each university hospital in Germany establishes a Data Integration Center (DIC), thus ensuring organizational, regulatory, and functional prerequisites while addressing interoperability and (re-)usability of data (Winter et al., 2018). During their treatment, patients can give consent for their data to be used in future research projects. Afterward, researchers can find and identify patient-related data and request data sets in a cross-organizational workflow, the Data Use and Access (DUA) process, thus addressing findability and accessibility of data.

The national commitment to a legal broad consent is a fundamental achievement of the MII (Medical Informatics Initiative, 2020), allowing for patient-related data to be processed and used in a determined and limited research context. Thus, the broad consent forms the basis and the first level of agreement to future secondary-purpose data usage given by each patient. Yet, it does not support transparency and consenting to specific research projects or a horizontal or vertical selection of data sets by patients. Therefore, the DUA process provides a second level of consent (Klötgen et al., 2021), realized as a vicarious and project-specific agreement based on individual regulations of the DICs.

The SMITH consortium develops the SMITH Service Platform (SSP), which provides common use cases and user interfaces (UI) for all connected DICs, such as the DUA process. Researchers submit a project-specific data usage proposal through the SSP, and the Data Use and Access Committee (UAC) of each involved DIC decides whether the requested data may be provided for the specific research project. In the end, the researcher and each DIC conclude a project-specific contract, allowing the requested data sets to be provided by the SSP. The DUA process is realized as a distributed process with a central process management (Klötgen et al., 2021), providing tasks for the necessary process control and integration of DIC's subprocesses, components, and actors.

In order to manage consents and digital identities, pseudonyms, and their relations, the MII consortia establish Trusted Third Parties (TTP) as essential building blocks of data processing workflows, including protection, pseudonymization, and anonymization of data. Many DICs will integrate the 'generic Informed Consent Administration Service' (gICS) as a tool to manage patients' broad consents (Rau et al., 2020). In this context, gICS allows requesting data sets of all consenting patients and it can be integrated into the real-time data processing tasks of a DIC. Yet, gICS does not support patients in constraining specific data donations for selected medical research projects.

### 2.3 International Data Spaces

Numerous technologies exist that are capable of transferring sets of data to a remote consumer. But when it comes to organizational requirements, such as privacy regulations, security requirements, and legal contracting behind the technical process, the scientific landscape becomes rather scarce on options. The International Data Spaces (IDS) provide an ecosystem for sharing data, which aims to cover all the issues previously mentioned (IDSA, 2019). The IDS Association (IDSA) provides standardized policy negotiation and attested state-of-the-art security guarantees, and it aims to provide usage control for shared data. The IDS infrastructure has the goal of letting data providers remain in control and keep the ownership of their data even after the data has been released to consuming parties.

The IDS consist of divisions, which focus on sharing data for a certain domain, such as the Medical Data Space. This medical-specific data space allows scientists to share and regulate data being relevant for

health studies. Furthermore, participants communicate via IDS Connectors (IDSA, 2019), which serve as components for transferring data among each other. These connectors are typically attested using Trusted Platform Modules or Trusted Execution Environments. Most IDS Connectors contain Apache Camel<sup>1</sup>, which is an open-source message routing framework (IDSA, 2019). Apache Camel has more than 200 different protocol adapters allowing to transform incoming and outgoing messages across protocol boundaries. As a security mechanism, each implementation of an IDS Connector must regularly pass a certification, which determines the level of trust and security achieved. In the context of IDS, three different security levels exist to handle ordinary communication as well as highly confidential data flows. The set of minimal trust levels and security requirements which need to be guaranteed by an IDS Connector is defined in a so-called IDS Policy. IDS Connectors must mutually agree on IDS Policies which contain requirements for security standards and rules for processing data flows. Furthermore, IDS Policies result in so-called IDS Contracts after successful negotiation. This negotiation is a specific IDS process to deposit IDS Contracts with IDS Policies on the recipient side (Hosseinzadeh et al., 2020).

### 2.4 Usage Control

Usage control is a research field that deals with the extension of traditional access control to enforce rules on data even after their release. Eitel et al. gave a suitable definition for the perspective of this topic:

"[Usage control] is about the specification and enforcement of restrictions regulating what must (not) happen to data. Thus, usage control is concerned with requirements that pertain to data processing (obligations) rather than data access (provisions). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management." (Eitel et al., 2021)

The idea of usage control was first formalized by Park and Sandhu with their model of UCON-ABC, which stands for usage control with definitions for authorizations, obligations, and conditions (Park & Sandhu, 2004; Sandhu & Park, 2003). By that time, classical access control was the prevalent paradigm, but it was unable to enforce access rights beyond the first provision of a user's access rights. For instance, one of the first implementations of usage control in a distributed system was proposed by Pretschner

<sup>1</sup> <https://camel.apache.org/> (last accessed: 2021/10/27)

(Pretschner et al., 2006). Afterward, the UCON-ABC was incrementally improved, implemented numerous times, and equipped with more expressive policy languages such as XACML and additional extensions, as it is the case for a tool like the MY DATA Control Technology<sup>2</sup>. IDSA also deals with usage control, defines standardized rules and a corresponding policy language for implementing such usage control mechanisms (Bader et al., 2020; Eitel et al., 2021; Hosseinzadeh et al., 2020). For instance, the previously mentioned MY DATA Control Technology can be used to enforce the rules in an IDS Connector.

### 3 CONCEPT

MII’s DUA process incorporates two levels of agreement to data usage. Acting as the data owner, a citizen provides a broad consent on the first level of agreement, thus approving the usage of medical data for the research in general. This enables researchers to find patients’ data managed by the specific DIC for usage within data use projects. Acting as the data provider, the UAC of a DIC approves a researcher’s data usage proposal and agrees or disagrees to the usage of each patient’s data vicariously on the second level of agreement. Due to the lack of transparency and influence for citizens regarding specific data use projects, we added a third level of agreement enabling citizens to constrain the usage of their data in the context of specific data use projects and thus, strengthening patient empowerment and data sovereignty. These three levels are represented in Figure 1 and form the starting point of our work.

Our concept comprises components and systems of the SMITH project such as SSP and DICs on the one hand, and IDS technology such as IDS Connectors and embedded usage control on the other hand. Hence, in our concept, we combine existing technologies from SMITH and IDS to create a portal focusing on the participation of patients.

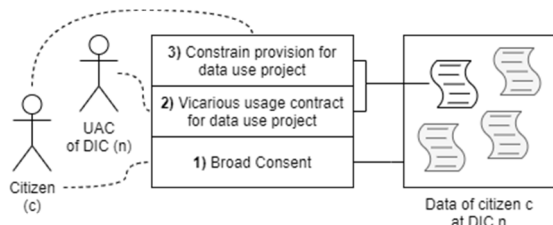


Figure 1: Levels of Agreement.

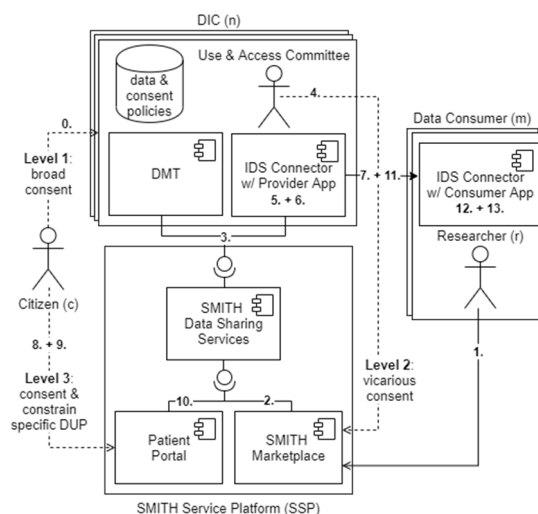


Figure 2: Concept Overview.

Figure 2 shows an overview of our concept, and the demonstrated scenario follows a chronological sequence with 14 steps, marked in the illustration.

Firstly, patients agree in the MII broad consent to donate their data for all interested medical research projects at the doctor’s appointment, as described before in the first level of agreement, and, in addition, they gain personal login details for the patient portal (0). After that, data is available, and researchers use the SMITH Marketplace to provide a data usage proposal containing a data query that is needed for the appropriate research (1). The Data Sharing Services component, acting as the central repository for data use projects and connecting component for multiple DICs, manage all workflow based interactions between involved actors and provide all tasks included in the DUA process (2). When a task addresses a DIC, its Data and Metadata Transfer Unit (DMT) is notified (3), which retrieves the necessary information and triggers a local subprocess. Thus, the UAC is able to manage and provide the individual evaluation of a data usage proposal (4). When the data use project is accepted, the Data Sharing Services provide data provision tasks to the involved DICs in the same way, and the requested data sets are sent to the provider app within the IDS Connector instance (5). Based on the research project conditions, an IDS Policy is created (6) and negotiated with the researcher’s IDS Connector (7). After the project policy is deployed, patients may intervene. The implemented patient portal shows project information and corresponding data processing to the patients (8),

<sup>2</sup> <https://www.dataspaces.fraunhofer.de/de/software/usage-control/mydata.html> (last accessed: 2021/10/19)

so the involved patients gain insights into the requesting projects and can decide to accept or to reject the requested data transfer, which forms the third level of agreement (9). The default setting represents consent to the requesting project by using the MII broad consent. If a patient rejects the data transfer for a selected project, no data is sent to the related researcher's IDS Connector, and, as a result, the researcher will not receive data from the declining patient. Otherwise, after a period the requested data is filtered using the IDS Policy (10) and subsequently securely sent (11). Within the IDS Connector of the researcher, data is also checked using the IDS Policy, for instance, by checking valid time intervals for usage and, after that verification, forwarded to the consumer app (12). Hence, IDS mechanisms support the enforcement of patient choices but transferred data cannot be withdrawn by patients. After a defined period for rejection, patient choices are final due to the required researchers' planning dependability. Finally, the consumer app will display the requested data to the researcher if the check of the IDS Policy was valid (13).

Our objective is to improve the ability of patients to be sovereign in their data donations for medical research. By using the IDS Connectors, a technology

focusing on fair data sharing and sovereign participants was chosen to achieve this objective. Patients can intervene in the transfer of data for specific research projects. Hence, patients can choose which projects they want to support with their data. This approach answers RQ1. A detailed description of the used components is presented in the following Section 4, answering to RQ2.

### 4 IMPLEMENTATION

A main objective of our work regarding usage control is to empower patients to keep control of their personal medical data. Another objective is to consider the time span of requesting research projects and to impose a time constraint on the visibility of the data on the researcher's side as an obligation, which must be automatically enforced. Thus, data usage control affects several steps in the process of transferring data. First, a DIC checks the authorization for accessing the patient data. This was already implemented on DICs by UAC and is not part of our implementation. After that and before sending the data, the consent or refusal of patients is is

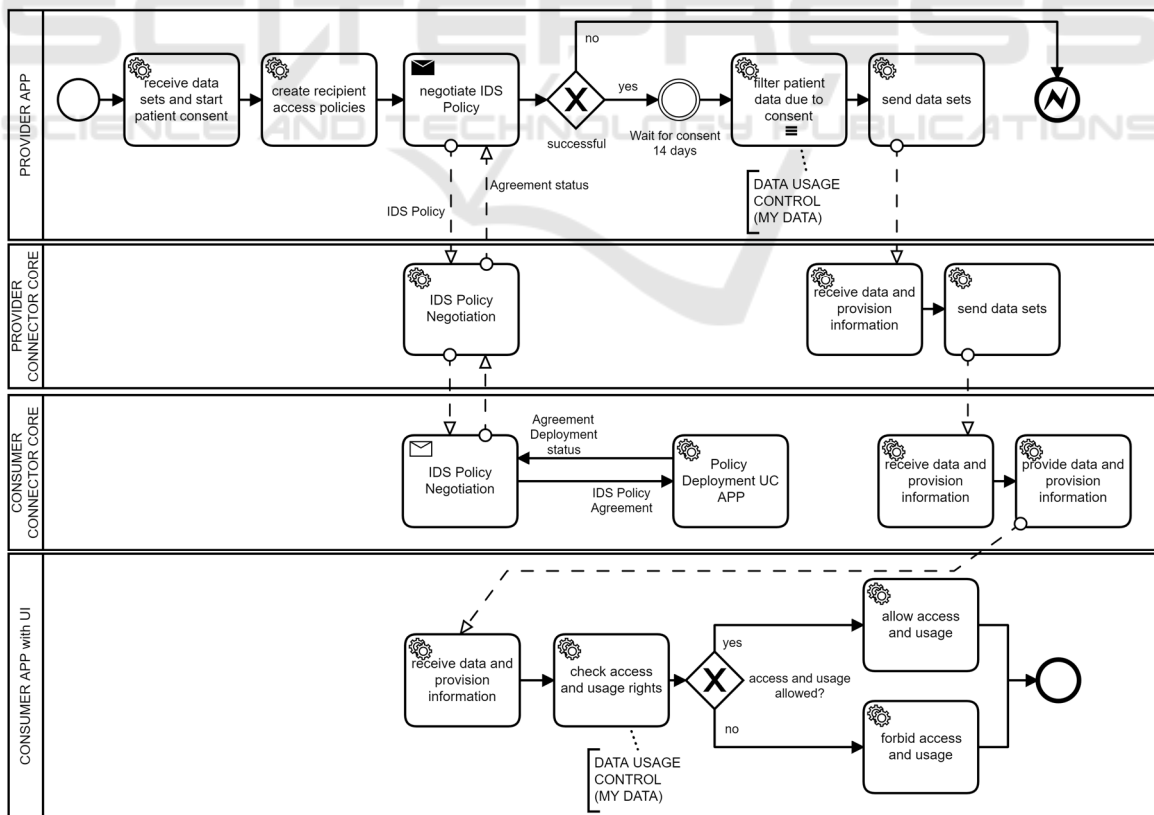


Figure 3: Business Process Model of Implementation.

considered in the data sets. Subsequently, IDS Policies are exchanged between IDS Connectors that include the duration of the project so that no data will be displayed after this time span. Figure 3 shows the process that implements our concept.

For our prototypal implementation, we use Trusted Connectors as a specialization of IDS Connectors (Schütte et al., 2018), which are open source and feature a high trust level. A Trusted Connector is a runtime environment. Its core component serves as a gateway for inbound and outbound network requests and communication between user apps running on it, for instance, consumer and provider apps (Schütte et al., 2018). Furthermore, MY DATA Control Technology is integrated using Camel Interceptors<sup>1</sup>. A Camel Interceptor is an integration pattern of the Apache Camel framework with the purpose of interrupting the original flow of messages and applying various actions to the messages and data. In addition, we have implemented connector apps on both the provider's side and the consumer's side, whose functionality is described in the following.

Starting on the provider's side, see top left of Figure 3, the provider app fetches the requested data sets from the DIC's storage. Those data sets are expressed in HL7 FHIR<sup>2</sup> format, where a FHIR Bundle<sup>3</sup> acts as a project, and FHIR Conditions<sup>4</sup> contained in a FHIR Bundle represent the medical data of specific patients. Subsequently, patients can view the available projects and their included own medical data for donation in a UI within the patient portal. Patients withdraw their consent for specific projects or retain their consent by broad consent. The authentication of patients in the patient portal is based on the patient login details which they received at the doctor's appointment before. Furthermore, the IDS Contracts with policies, which are generated by our prototype, are 'negotiated' with the recipient over the period of use, matching the requested duration of the project. Patients have 14 days to withdraw their consent. The prototype implements this mechanism with a time-based event. After that, the provider transforms the originally fetched data sets, filtering out the medical data of patients who decided to withdraw their consent. As next step, the provider transmits the altered data sets—only after successful IDS Contract negotiation—via the provider's core

component of Trusted Connector to the consumer's core component of another Trusted Connector.

The altered data sets are now arriving on the consumer's side. Since the data sets possess a unique identifier as an attribute of the FHIR Bundle, they can be referenced by the IDS Policies. Before the data is passed to the consumer app, where the researcher will be able to view the potentially altered data sets tabularly in a UI, MY DATA Control Technologies check the corresponding time-based rules for the project. The rules are also checked before each display in the UI, so the data will only be visible within the consumer app for the duration of the project and can also no longer be transferred within the IDS Connector. In addition, the flow of messages in the connector is defined by so-called Camel Routes<sup>5</sup>. On these Camel Routes, the Camel Interceptor is applied to control the flow of messages.

In summary, our implementation points out that a close dovetailing between technology and contracts is required. The IDS provide data exchange mechanisms that guarantee a high level of policy enforcement. These components are relevant for a valid implementation of our concept, which answers RQ2. Furthermore, our added elements, such as the patient portal and the integration of three levels of agreement, are also part of an answer to RQ2.

## 5 DISCUSSION

Our concept and implementation demonstrate sovereign data donation in medical research. Furthermore, our work provides benefits for all participants in the data donation process. The results could also be beneficial for future work towards a European strategy for data spaces, since IDS provides a potential foundation of Gaia-X (Otto et al., 2021).

Firstly, we show an opportunity for patients to donate their medical data sovereignly by combining existing technology with additional elements. This result answers RQ1, defined in Section 1. Further, using our patient portal leads to a sovereign patient empowerment and fosters trust in donating medical data. Providing patients with choices of specific research projects for their medical donation strengthens patients' trust because of the secure

<sup>1</sup> <https://camel.apache.org/components/3.11.x/eips/intercept.html> (last accessed: 2021/10/27)

<sup>2</sup> <https://www.hl7.org/fhir/> (last accessed: 2021/10/27)

<sup>3</sup> <https://www.hl7.org/fhir/bundle.html> (last accessed: 2021/10/28)

<sup>4</sup> <https://www.hl7.org/fhir/condition.html> (last accessed: 2021/10/28)

<sup>5</sup> <https://camel.apache.org/manual/routes.html> (last accessed: 2021/10/28)

implementation and enforcement of their individual choices in a technical way by our developed system.

Secondly, our approach is based on data in HL7 FHIR format. Therefore, our work is interoperable with several other existing medical tools and systems, using the same international standard. Hence, our work contributes to a comprehensive data availability due to the interconnection of numerous data sources, such as DIC or other medical and clinical data storages. The implementation is based on components by MII, SMITH, IDS, and MY DATA Control Technologies, so we point out an interplay of these different components. Therefore, by adding specific new components, our concept implementation approach responds to RQ2.

Finally, extending IDS technology with aspects involving citizens moves the rather industrial focus further to a more general application. So far, IDS have been used mostly in corporate and scientific contexts. Since our approach describes a patient embedding, citizens can participate in data ecosystems from now on. It must be noted that citizens do not use their own IDS Connectors, but they can interact with a portal allowing them to adjust data donation flows. These settings are transformed into machine-readable policies that are embedded into the IDS Connectors of DICs and researchers. This procedure enables citizens to participate in data donation in particular and in data sharing processes in general. However, there are still limitations on data usage for analysis purposes in external systems. The policy enforcement no longer exists if data leaves the IDS Connector, but this does not relieve data consumers of their legal obligations to comply with the contract. However, there are two promising approaches enabling technical enforcement. On the one hand, the development of special IDS applications with appropriate analysis functions embedded into the Connector, and on the other hand, the extension of existing applications with data usage mechanisms.

## 6 CONCLUSION AND OUTLOOK

We conceptualized and implemented an initial approach, empowering patients to make sovereign data-donating decisions. For this objective, we combined the MII broad consent concept with components from the IDS and MY DATA Control Technologies to create new opportunities for patients to control the use of their data. Our concept is based on patients' broad consent given during medical treatment. Broad consent allows donating medical data for medical research, but patients cannot choose

specific research projects. We argue that patients must become more involved in the data donation process for medical research. To this end, we developed a system empowering patients to make sovereign decisions about donating their medical data to specific medical research projects. As a result, we contribute to sovereign medical data donation considering individual patients. Additionally, with our system based on industrial technologies such as IDS and MY DATA Control Technologies, we contribute to (industrial) data ecosystems considering not only companies but also individuals' preferences.

Since we developed an initial prototype, our research is limited in terms of application in common practice. Further research should validate our prototype with patients donating medical data and researchers requesting medical data. Furthermore, our approach can further enhance patients' data sovereignty, for instance, by enabling patients to select specific data types for their donation to specific medical research projects.

## REFERENCES

- Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, 21(2), 262–282. <https://doi.org/10.7454/global.v21i2.412>
- Bader, S., Pullmann, J., Mader, C., Tramp, S., Quix, C., Müller, A. W., Akyürek, H., Böckmann, M., Imbusch, B. T., Lipp, J., Geisler, S., & Lange, C. (2020). The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content. In J. Z. Pan (Ed.), *Lecture Notes in Computer Science: Vol. 12507. The Semantic Web - ISWC 2020: 19th International Semantic Web Conference* (Vol. 12507, pp. 176–192). Springer. [https://doi.org/10.1007/978-3-030-62466-8\\_12](https://doi.org/10.1007/978-3-030-62466-8_12)
- Bild, R., Bialke, M., Buckow, K., Ganslandt, T., Ihrig, K., Jahns, R., Merzweiler, A., Roschka, S., Schreiweis, B., Stäubert, S., Zenker, S., & Prasser, F. (2020). Towards a comprehensive and interoperable representation of consent-based data usage permissions in the German medical informatics initiative. *BMC Medical Informatics and Decision Making*, 20(1), 103. <https://doi.org/10.1186/s12911-020-01138-6>
- Caulfield, T., & Kaye, J. (2009). Broad Consent in Biobanking: Reflections on Seemingly Insurmountable Dilemmas. *Medical Law International*, 10(2), 85–100. <https://doi.org/10.1177/096853320901000201>
- Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Eitel, A., Jung, C., Brandstädter, R., Hosseinzadeh, A., Bader, S., Kühnle, C., Birnstill, P., Brost, G., Gall, M., Bruckner,

- F., Weißenberg, N., & Korth, B. (2021). *Usage Control in the International Data Spaces*. Dortmund Berlin. International Data Spaces Association.
- European Parliament and Council of European Union. (2016). *Regulation (EU) 2016/679*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>
- Hosseinzadeh, A., Eitel, A., & Jung, C. (2020). A Systematic Approach toward Extracting Technically Enforceable Policies from Data Usage Control Requirements. In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)* (pp. 397–405). <https://doi.org/10.5220/0008936003970405>
- IDSAs. (2019). *Reference Architecture Model: Version 3.0 | April 2019*. International Data Spaces Association. <https://internationaldataspaces.org/use/reference-architecture/>
- Klötgen, M., Fiege, E., & Houta, S. (2021). Concept and Implementation of Data Usage Proposal Process Based on International Standards in SMITH. *Studies in Health Technology and Informatics*, 278, 171–179. <https://doi.org/10.3233/SHTI210066>
- Lauf, F., Scheider, S., Meister, S., Radic, M., Herrmann, P., Schulze, M., Nemat, A. T., Becker, S. J., Rebbert, M., Abate, C., Konrad, R., Bartsch, J., Dehling, T., & Sunyaev, A. (2021). *Data Sovereignty and Data Economy—Two Repulsive Forces? Position Paper*. Dortmund. Fraunhofer Institute for Software and Systems Engineering ISST. <https://doi.org/10.24406/issst-n-634865>
- Medical Informatics Initiative. (2020). *Template text for patient consent forms*. <https://www.medizininformatik-initiative.de/en/template-text-patient-consent-forms>
- Meister, S., & Otto, B. (2019). *Digital Life Journey: Framework for a self-determined life of citizens in an increasingly digitized world (basic research paper)*. Dortmund. Fraunhofer Institute for Software and Systems Engineering ISST. <https://doi.org/10.24406/ISSST-N-559377>
- Ohmann, C., Banzi, R., Canham, S., Battaglia, S., Matei, M., Ariyo, C., Becnel, L., Bierer, B., Bowers, S., Clivio, L., Dias, M., Druml, C., Faure, H., Fenner, M., Galvez, J., Gherzi, D., Gluud, C., Groves, T., Houston, P., . . . Demotes-Mainard, J. (2017). Sharing and reuse of individual participant data from clinical trials: Principles and recommendations. *BMJ Open*, 7(12), e018647. <https://doi.org/10.1136/bmjopen-2017-018647>
- Otto, B. (2016). *Digitale Souveränität: Beitrag des Industrial Data Space*. Munich. Fraunhofer Institute for Software and Systems Engineering ISST. <https://doi.org/10.13140/RG.2.2.35125.68321>
- Otto, B., Rubina, A., Eitel, A., Teuscher, A., Schleimer, A. M., Lange, C., Stingl, D., Loukipoudis, E., Brost, G., Böge, G., Pettenpohl, H., Langkau, J., Gelhaar, J., Mitani, K., Hupperz, M., Huber, M., Jahnke, N., Brandstädter, R., Wessel, S., & Bader, S. (2021). *Gaia-X and IDS*. Berlin. International Data Spaces Association. <https://doi.org/10.5281/zenodo.5675897>
- Park, J., & Sandhu, R. (2004). The UCON ABC usage control model. *ACM Transactions on Information and System Security*, 7(1), 128–174. <https://doi.org/10.1145/984334.984339>
- Posch, R. (2017). Digital sovereignty and IT-security for a prosperous society. In H. Werthner & F. van Harmelen (Eds.), *Informatics in the Future* (pp. 77–86). Springer. [https://doi.org/10.1007/978-3-319-55735-9\\_7](https://doi.org/10.1007/978-3-319-55735-9_7)
- Pretschner, A., Hilty, M., & Basin, D. (2006). Distributed usage control. *Communications of the ACM*, 49(9), 39–44. <https://doi.org/10.1145/1151030.1151053>
- Rau, H., Geidel, L., Bialke, M., Blumentritt, A., Langanke, M., Liedtke, W., Pasewald, S., Stahl, D., Bahls, T., Maier, C., Prokosch, H.-U., & Hoffmann, W. (2020). The generic Informed Consent Service gICS®: Implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research. *Journal of Translational Medicine*, 18(1), 287. <https://doi.org/10.1186/s12967-020-02457-y>
- Sandhu, R., & Park, J. (2003). Usage control: A vision for next generation access control. In *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*. Symposium conducted at the meeting of Springer.
- Schütte, J., Brost, G., & Wessel, S. (2018). *Der Trusted Connector im Industrial Data Space*. Garching. Fraunhofer Institute for Applied and Integrated Security AISEC. [https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien\\_TechReports/deutsch/IDS-Paper\\_Datensouveraenitaet.pdf](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/IDS-Paper_Datensouveraenitaet.pdf)
- Semler, S. C., Wissing, F., & Heyder, R. (2018). German Medical Informatics Initiative. *Methods of Information in Medicine*, 57(S 01), e50–e56. <https://doi.org/10.3414/ME18-03-0003>
- Sheehan, M. (2011). Can Broad Consent be Informed Consent? *Public Health Ethics*, 4(3), 226–235. <https://doi.org/10.1093/phe/phr020>
- Specht-Riemenschneider, L., & Radbruch, A. (2021). Datennutzung und -schutz in der Medizin: Forschung braucht Daten. *Deutsches Ärzteblatt*, 118(27-28), 1359–1361. <https://www.aerzteblatt.de/int/article.asp?id=220270>
- Steinmüller, W., Lutterbeck, B., Mallmann, C., Harbot, U., Kolb, G., & Schneider, J. (1972). Grundfragen des Datenschutzes. In *Anlage zu BT-Drucks. VI/3826*.
- Wilkinson, M., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., Da Silva Santos, L., Bourne, P., Bouwman, J., Brookes, A., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C., Finkers, R., . . . Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*.
- Winter, A., Stäubert, S., Ammon, D., Aiche, S., Beyan, O., Bischoff, V., Daumke, P., Decker, S., Funkat, G., Gewehr, J. E., Greiff, A. de, Haferkamp, S., Hahn, U., Henkel, A., Kirsten, T., Klöss, T., Lippert, J., Löbe, M., Lowitsch, V., . . . Löffler, M. (2018). Smart Medical Information Technology for Healthcare (SMITH). *Methods of Information in Medicine*, 57(S 01), e92–e105. <https://doi.org/10.3414/ME18-02-0004>
- World Economic Forum. (2011). *Personal Data: The Emergence of a New Asset Class*. Geneva, CH. [http://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf)