The Data Donation Pass:
Enabling Sovereign Control of Personal Healthcare Data

Matthieu-P. Schapranow, Janos Brauer, and Hasso Plattner
Hasso Plattner Institute, Enterprise Platform and Integration Concepts,
August-Bebel-Str. 88, 14482 Potsdam, Germany
E-Mail: {schapranow|platter}@hpi.de, janos.brauer@student.hpi.de

Abstract—Today, anybody is able to create and collect more and more data for monitoring the personal health, e.g. by using smart or wearable devices. However, these data are stored in distributed data silos in heterogeneous formats operated by different service providers. Although, these data is considered as very helpful for researchers and medical experts, it is mostly inaccessible for them.

In the given contribution, we introduce the data donation pass, which enables citizens the sovereign control of their personal healthcare data in a digital society. It provides a holistic view of personal healthcare data independent from data source and data format. Furthermore, it enables the donation of selected subsets of de-identified data, e.g. for selected research projects, participation in clinical trials, or for supporting disease-specific longitudinal databases.

Keywords: Sovereign Control, Data Donation, Healthcare Data, Medical Innovations, Research, Digitalization

1. Introduction

The digital transformation is a current trend affecting more and more fields of our daily life, e.g. work, leisure, and healthcare [1]. Having more and more digitalized data in the field of healthcare at hand builds the foundation for precision medicine and fuels expectations of medical experts to improve existing healthcare process, identify disease roots, and develop better treatments [2], [3], [4], [5].

At the same time, data privacy becomes more and more important for sensitive healthcare data, e.g. in the U.S. Health Insurance Portability and Accountability Act or the German E-Health law [6], [7]. Today, data privacy is implemented through specific skilled data privacy officers and legal experts, which aim to protect personal information. However, in this setting the citizen, who is described by the acquired data, is still not asked.

In the given position paper, we introduce the data donation pass of the Analyze Genomes platform: an application for mobile and Internet-connected devices [8], [9]. The data donation pass as depicted in Figure 1 is a innovative approach to bridge the gap between healthcare professionals, industry, and researchers on the one hand side and informed citizens on the other side, who are willing to control their personal healthcare data.

Fig. 1: Screenshot of the Data Donation Pass application running on a smart phone device showing a notification about a specific clinical trial.
data, manage take their personal decisions, and support individual projects through donation of their personal healthcare data.

The remainder of the contribution is structured as follows: In **section 2** the ongoing trend of digital transformation is introduced whilst its impact on healthcare business models is outlined in **section 3**. The importance of data sovereignty in context of digital transformation is depicted in **section 4** whilst selected aspects of our contribution are outlined in **section 5**. We evaluate the applicability of our approach in **section 6** using selected real-world use case followed by a conclusion of our work in **section 7**.

### 2. Digital Transformation

The digital transformation builds the foundation for services of the 21st century by improving business processes within the entire society [10]. Within the manufacturing industry it is referred to the next stage of automation as "Industry 4.0" [1]. For example, it reduces media breaks, eliminates time-consuming manual process steps, and interconnects more and more actors and knowledge bases to facilitate meaningful insights. The digital transformation demands large enterprises as well as small- and mid-sized enterprises, but in healthcare, it affects every one of us equally.

How can we remain the master of the situation in the future without forgoing the advantages of fully digitalized healthcare processes? This is a concrete example for informed citizens, who need to be able to sovereign control their personal healthcare data anywhere at any time.

### 3. Healthcare as Business Model

Healthcare has become a bestseller in the recent years. Amongst others, large electronic and IT companies, such as Apple, Google, Microsoft, SAP, have recognized this emerging trend [11], [12]. As a result, a variety of consumer products have been released to the end-consumer market, e.g. to collect and monitor sleeping periods, workouts, body weight, even personal eating habits.

The combination of healthcare data, their analysis, and the discovery of universal regularities is the task of researchers all over the globe. However, especially researchers complain about lacking access to real-world data in a sufficient amount, precision, and quality, e.g. in clinical and pharmaceutical research [13].

Nonetheless, personal healthcare data are considered as sensitive data, which require specific protection. Therefore, discussion about data privacy of healthcare data are continuing around the globe without involving the relevant actor: the individual citizens [14]. And so we continue to perform electronic document and self-measurement. However, the so acquired data are stored in data silos operated by large global acting companies, shielded from third-party access, and protected by data privacy officers even from whom?

At the same time, parallels to George Orwell’s novel "1984" arise and fears of a transparent citizen, who is no longer able to live a self-determined life, are fanned [15]. However, this is neither a novel nor science fiction, it is boon and bane of a digital world in which we already live today. Therefore, we all as society members need to take personal responsibility to form the digital transformation in a way that on the one hand fears are understood and addressed and on the other hand benefits outperform potential risks.

### 4. Data Sovereignty as a Chance

In contrast to Orwell’s novel, we can actively contribute to how the digital transformation affects our lives. Therefore, we introduce the data donation pass as one particular option of determination in context of personal healthcare and healthcare data. It allows documenting and managing personal declarations of intent focusing on personal healthcare data comparable to the organ donation pass.

In contrast to the traditional paper-based version of the organ donation pass, we developed the data donation pass for the requirements of an entirely digitalized healthcare market. Thus, the data donation pass can be installed and used on smartphones and any Internet-connected personal devices in a similar way. Therefore, users of the data donation pass can document their personal consent anytime and anywhere. Furthermore, all given consents can be revoked at any later point in time without the need to name specific reasons. Revoking the access to personal files will stop exposing any additional details for future use. However, it does not affect earlier released and exposed data as these data might have already been used by the accessing party, e.g. in context of a scientific publication, which makes it impossible to hide them retrospectively.

In contrast to the organ donation pass, the data donation pass is of certain importance during lifetime, e.g. to grant medical specialists or family members access to specific healthcare data for specific purposes. Furthermore, it can also be used to express the personal will to donate all personal health records after death, e.g. for research purposes.

### 5. The Data Donation Pass

In the following, we will share a concrete example and demonstrate how the data donation pass is used. In the following example, all names, characters, and incidents portrayed are fictitious and no identification with actual persons (living or deceased), places, buildings, and products is intended or should be inferred.

Let us consider our persona: Stephanie is 27 years old and lives currently in Berlin, Germany. She suffers from a chronic heart insufficiency. With her chronic disease, Stephanie belongs to a group of up to approx. two percent of all U.S. Americans and a group of approx. 300,000 newly diagnosed Germans per year suffering from a form...
of heart failure [16, 17]. Since Stephanie cares about her personal health, she schedules regular appointments with her cardiologist to monitor her individual heart function. During her doctor visits, specific lab parameters are acquired to document Stephanie’s disease at a certain point in time. Documenting the same lab parameters over time results in a longitudinal data set. With the help of these longitudinal data, researchers can analyze details about the progress of Stephanie’s disease and predict trends using statistical data models [18]. Stephanie hopes that in future there will be an alternative therapy form available in addition to the traditional drug-based therapy. Therefore, she is interested to support heart insufficiency research with her personal cardiology data.

5.1 Installation and Configuration

The data donation pass can either be used via a website-based User Interface (UI) or via apps designed for mobile devices and smartphones. The data donation pass can be accessed by either UI via the exposed Application Programming Interface (API). Data is exchanged between the backend server and the UI using Asynchronous JavaScript And XML (AJAX) calls encapsulating payload data in a specific JSON communication protocol, which is carried via encrypted HTTPS connections [19, 20, 21].

Users of the data donation pass application need to register a personal user account prior their first use to create their personal health record on the backend system [3]. The personal user account is protected by a personal username and password. After registration users need to verify their personal account using details from your health insurance card and link them [22]. Amongst others, you can manage granted access rights, manage personal data privacy rules, access personal healthcare data, and configure personal fields of interests after logging into your personal user account of the data donation pass.

5.2 Using the App

Stephanie uses the mobile application of the data donation pass on her smartphone as depicted in Figure 1. After downloading and installing the app on her smartphone, Stephanie added chronic heart insufficiency as one of her personal field of interest in her user account. By adding fields of interest she agrees to receive personal notifications about these topics in regular times comparable to e-mail newsletters. As a result, Stephanie receives latest details about her chronic heart disease, e.g. latest medical advances, new research publications, and latest research projects.

We meet Stephanie on her way to work when she receives a notification in the news tab of the app on her smartphone as depicted in Figure 1. An international research consortium is performing a clinical trial for an innovative treatment for cardiomyopathy patients like her, which is able to manage the disease in a more advanced way whilst reducing the total amount of required pills per day. "That appears to be very relevant for me", says Stephanie and selects the "Interested" button within the data donation app.

5.3 Informed Consent

After Stephanie’s expression of interest, the practice of her cardiologist receives automatically further medical details of the clinical trial. Thus, Stephanie’s cardiologist will be able to conduct a detailed therapy talk about the proposed program and Stephanie will be able to discuss any open questions. Stephanie decided to participate in the proposed research project and signed the informed consent in the practice of her local medical expert. As a result, members of the research project are granted access to relevant medical parameters of Stephanie’s Electronic Medical Record (EMR) and her anamnesis at her cardiologist.

Relevant parameters for the research project are processed prior to their release to the research project. In this data de-identification process identifying attributed are substituted by pseudonyms to protect Stephanie’s identity [23]. Members of the research project have access to real-word data whilst Stephanie’s personal identity remains protected during her participation. In case of critical findings, the data donation pass can also be used to contact the real-world individual behind the pseudonyms and to share crucial details with medical experts.

5.4 Transparency

In addition, Stephanie can access the same data, which are also provided for the research project. As a result, Stephanie feels even more informed about her disease through her personal involvement in the research project as she is able to view and access her personal parameters at any time of her program participation. Furthermore, she receives regular updates about her program participation, e.g. which of her parameters were accessed how often. This shows Stephanie how important her data donation is for the success for the research project, which is considered as an important feedback method to improve participation compliance [24].

6. Evaluation and Discussion

In the following, the applicability of the presented data donation pass is evaluated using selected real-world use cases. Due to page restrictions, we discuss each use case in brief in the following.

6.1 Chronic Disease Management

Consider yourself suffering from a chronic disease, such as diabetes, asthma or heart failure as outlined in section 5. You will have regular doctor appointments to document the progress of the disease and the success of the selected therapy in a longitudinal form, e.g. in context of specific disease management programs [25]. However, you will have
barely access to data of companions with a similar anamnesis to understand your personal progress and assess your personal performance compared to the cohort of patients like you. Today, researchers need to conduct prospective studies, which involves, amongst others, the recruitment of participating persons in a research program and the acquisition of data. As a result, prospective studies are considered as time-consuming and complex [18].

The data donation pass allows the self-determined donation of selected personal healthcare data, e.g. to support research projects. By donating your personal healthcare data through the data donation pass, citizens can contribute to a form disease-specific longitudinal research database. As a result, researchers will be able to perform retrospective research, i.e. the secondary use of existing data with the explicit consent from the data givers. With the help of such research databases, researchers will have access to de-identified real-world data of representative disease-specific cohorts to study, amongst others, populations, civilization diseases, and assess the quality of current treatment approaches in context of health services research. The research database can also be used as real-world reference to interpret the disease and the personal progress compared to a cohort of people with a similar anamnesis. This also provide the prevention of possible risk factors, e.g. co-morbidities or severe events documented by other people. As a results, medical doctors will be able to build their treatment decision on the experiences of a huge patient cohort, which they do not have access to as of today.

6.2 Geriatric and Child Care

The age structure of most industrial countries has changed over the past decades. On the one hand, the birthrate stagnates or even declines in most countries. On the other hand, the average life expectancy raises, e.g. thanks to access to improved healthcare services or healthier diet [26]. As a result, a growing fraction of the elderly society requires long-term geriatric care, which also includes support from own family members, e.g. from adult children. In addition to this demographic aging, also parents need to manage regular medical appointments and consultations for their own children, e.g. when they suffer from chronic diseases or age-specific vaccinations are due. Both examples require caring persons to keep pace with and manage an ever-increasing amount of data.

The data donation pass allows the definition of trusted persons, e.g. to grant custody to your own children or other family members. As a result, specified trusted person receive access to selected private data similarly as they would be their personal healthcare data. Thus, caring family members can use the data donation pass also to form a holistic view on healthcare data of persons they take care of, e.g. to check for regular appointments, required pharmaceutical, or medical check-ups. The process of acquiring and maintaining healthcare data becomes more structured than having a folder full of paper-based medical documents at home. As a result, it also allows the definition of specific on-demand services upon these data sources, which should focus on benefits for their users. As a result, citizens interviews indicate that these services should extend or built upon existing services without the need to provide completely new services, e.g. calendars, e-mail notifications, or appointment scheduling [27].

6.3 Individual Clinical Trials

Innovative pharmaceutical products need to proof risk and chances in different stages of clinical trials prior to their market release [28]. Today, candidates for clinical trials need to be identified during the pre-screening phase of the clinical trial. Therefore, the matching of patient-specific data with study-specific inclusion and exclusion criteria is conducted. However, it involves time-consuming and manual analysis of individual trial criteria for hundreds of thousands of patient profiles [29]. As of today, the identification of candidates is rarely structured and builds mainly on untargeted methods, such as advertising in TV spots, newspapers, public transports or online marketing.

The data donation pass establishes for a first time a direct communication channel between interested and motivated candidates and Clinical Research Organizations (CROs) whilst keeping the identity of candidates protected. As a first step, interested users have to donate their healthcare care data to a research database pool. Approved research projects are allowed to access the relevant subset of de-identified data within the research database to perform their required tasks, e.g. filter for relevant candidates. In the given use case, a clinical research organization would use certain available attributes to pre-check inclusion and exclusion criteria for specific clinical trials. Through the integrated notification system, a brief message about the clinical trials can be send out to the group of candidates if they enabled notifications in their personal user profile. If candidates are interested in learning more about the project, they can directly indicate their interest in the data donation pass. As a result, details about the treating medical doctor will be provided to the CRO, who will send in response details about the clinical trial to allow her or him an informed consent discussion in a private setting with the patient.

7. Conclusion

In the given contribution, we shared details about our data donation pass. We consider it as a powerful way of active citizen participation in context of the ongoing digital transformation in healthcare. An open-minded discussion about and the meaningful use of digital healthcare data enables completely new perspectives for citizens, patients, and researchers. However, the example of the data donation pass also shows the need for an enlightenment of citizens
as foundation for a success digital transformation in the healthcare sector.

As a result, we propose an early education in digital technologies, e.g. as part of specific courses in primary school, as well as constant live-long learning offerings, e.g. using massive open online courses. In future, every one of us needs to be able to conduct personal informed and sovereign decisions about whether and if yes which of the personal healthcare data should be used for which particular use. Nonetheless, it is important to guarantee the same quality of healthcare services for all citizens. For example, if people decide actively not to participate in digitalized processes, they should receive the same quality of services and no disadvantages compared to citizens actively supporting the digital transformation.

The data donation pass is a very concrete example focused on the requirements of human beings for how out of abstract discussions around the topic data privacy in healthcare very specific and practical solutions arise. It demonstrates impressively how informed citizen can get access to their personal healthcare data whilst being able to manage and control access rights to them. As a result, we believe that generic data privacy discussions can be transformed in actions by directly involving individuals.

References


