Privacy Mental Models of Electronic Health Records: A German Case Study

Rebecca Panskus, *Ruhr-University Bochum;* Max Ninow, *Leibniz University Hannover;*
Sascha Fahl, *CISPA Helmholtz Center for Information Security;*
Karola Marky, *Ruhr-University Bochum and Leibniz University Hannover*

https://www.usenix.org/conference/soups2023/presentation/panskus

This paper is included in the Proceedings of the
Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Privacy Mental Models of Electronic Health Records: A German Case Study

Rebecca Panskus[1], Max Ninow[2], Sascha Fahl[3], Karola Marky[1,2]
[1]*Ruhr-University Bochum, Germany,* [2]*Leibniz University Hannover, Germany*
[3]*CISPA Helmholtz Center for Information Security, Germany*

Abstract

Central digitization of health records bears the potential for better patient care, e.g., by having more accurate diagnoses or placing less burden on patients to inform doctors about their medical history. On the flip side, having electronic health records (EHRs) has privacy implications. Hence, the data management infrastructure needs to be designed and used with care. Otherwise, patients might reject the digitization of their records, or the data might be misused. Germany, in particular, is currently introducing centralized EHRs nationwide. We took this effort as a case study and captured the privacy mental models of EHRs. We present and discuss the findings of an interview study where we investigated expectations towards EHRs and perceptions of the German infrastructure. Most participants were positive but skeptical, yet expressed a variety of misconceptions, especially regarding data exchange with health insurance providers and read-write access to their EHRs. Based on our results, we make recommendations for digital infrastructure providers, such as developers, system designers, and healthcare providers.

1 Introduction

Centralized electronic health records (EHRs) bear the potential for providing better patient care [16], for instance, by having more accurate diagnoses, improved patient safety [32,42], and cost reduction [18]. Some countries deploy such centralized infrastructures, such as the UK [36], Denmark, or Australia.Yet, despite the apparent benefits, most countries do not have a digital infrastructure. Hence, sensible and important health-related data must be shared between healthcare practitioners, mostly by the patients. Introducing central, nationwide digitization of health-related data requires care. Otherwise, (a) patients might not adopt using the digital infrastructure [31,34] or (b) the digital infrastructure might be misused by malicious actors [6].

Research has repeatedly shown that privacy perceptions of patients play an integral role in the context of EHRs [22, 30,34]. Specific concerns included unauthorized access [30], misuse of data [31], or increased health insurance costs for patients with certain health conditions [5,22,22,30,31].

In this paper, we investigate the specific use case of Germany, where the Federal Ministry of Health introduced national EHRs in January 2021 [21]. Germany uses an infrastructure that turns health insurance companies into providers of EHR access apps. However, they can only access specific data, which introduces challenging trust assumptions toward insurance companies. So far, using EHRs is voluntary for patients, and most German citizens are not even aware of EHRs, yet many informed individuals would like to use it [1]. Further, Germany's health infrastructure has a unique feature: Access to the centrally stored EHRs is controlled through mobile apps provided by health insurance companies [21] resulting in 85 different apps [23].

To contribute a part in evaluating the understanding and acceptance of German citizens towards EHRs, we first took a look at the mental models of individuals, which are internal representations that humans derive from the real world, e.g., how and why a technology works [25]. In related domains, such as the IoT, mental models profoundly impact adopting systems that handle sensitive health data [5,34]. This motivates our first research question:

RQ1: Which mental models do patients have regarding EHRs? – We specifically focus on privacy, data access, and trust including expectations about data handling.

Since the correctness of mental models also impacts adoption and usage intention [25], we specifically investigate misconceptions:

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

RQ2: What are patients' misconceptions of the EHR? – We specifically focus on the German EHR infrastructure.

Finally, we investigate risk perceptions of individuals:

RQ3: Which risks do patients perceive in the EHR context? – We specifically focus on the German EHR infrastructure.

To answer the above research questions, we conducted semi-structured interviews with 21 participants that included drawing mental models of the expected German infrastructure. We also confronted participants with the actual national infrastructure to capture their perceptions.

Our results show that the participants consider health insurance companies to play a central role. However, we identified many misconceptions about that role that mostly originate from misconceptions already in the analog world. For instance, participants mistakenly thought that health insurance companies had detailed access to all patient data. Patients critically viewed the fact that health insurance companies, on the one hand, provide the apps to control EHRs, yet are, on the other hand, not allowed or should not be allowed to access all patient data. Most participants also considered it to have a rather negative impact that patients in Germany are allowed to add and delete documents. We demonstrate further expectations and misconceptions of the patients focusing on trust and privacy. Based on our findings, we leverage the lessons learned from this use case to inform infrastructure design, data handling, and access to EHR infrastructures.

Research contributions: In the course of this paper we make the following contributions:

1. **First mental model investigation of German EHR:** We present the first investigation of user perceptions of the German EHR. We specifically investigate the privacy mental models of 21 participants through semi-structured interviews and a drawing exercise.
2. **Analysis of perceived risks, expectations & misconceptions:** Among our results, we show perceived risks, misconceptions, and expectations towards EHR highlighting challenges arising from health insurance companies' unique role in the German infrastructure.
3. **Overall recommendations for EHRs:** We conclude with recommendations for digital infrastructure providers, such as developers, system designers, and healthcare providers. We further provide viable lessons learned from the German use case.

2 Background & Related Work

Electronic health records (EHRs) have several advantages compared to their analog counterpart, especially in terms of availability, completeness, and accessibility for different authorized stakeholders, the digital version presents a better solution for patients. There are two main ways to digitize patient records: (1) EHRs, as detailed above, and (2) personal EHRs managed by the patients (PEHRs), e.g., having the data on a USB drive. In this section, we first introduce the German infrastructure to store and access EHRs as defined by the Federal Ministry of Health [21]. Then, we detail related work on mental models, privacy, and investigations of (P)EHRs.

2.1 German Infrastructure

The German EHR was introduced in 2022 by the Patient Data Protection Act, which obliges all health insurance companies to provide all insured persons with an EHR upon request from the beginning of 2021.

Health Insurances in Germany: To understand the German infrastructure, we first need to provide information about German health care. Germany has two types of health insurance: (1) statutory health insurance companies and (2) private ones. Patients insured by statutory health insurance companies pay contributions calculated based on their income. Compared to that, the contributions for private health insurance depend on the age and the health of patients when they enter their contract. For statutory insured patients, their health insurance company pays most costs directly to the health care providers. Privately insured patients pay the health care providers themselves and get reimbursed from the insurance. In both cases, health insurances get a) the doctor ID, b) received treatment (incl. diagnosis & billing codes), and c) data to identify the patient [39], which is legally defined in German law. Consequently, health insurances have to follow binding rates that are specified nationwide. From a privacy perspective, the health insurance company cannot get more detailed information, and the received information can be used for billing purposes.

Data: The data is stored on a central server managed by *Gematik*, the National Agency for Digital Medicine. Patients can store their emergency data, medication plans, doctor's letters, findings, or X-rays in their EHR. They can also upload their data, e.g., their blood glucose diary. All data stored is protected by encryption. Patients can also delete data at any time. The data is lost if doctors do not have the data stored locally in their doctor's office.

Availability / Access: The EHR is available for patients that have an electronic health card. Those cards are distributed by statutory health insurance. Mobile device apps can manage the data access on a (1) smartphone, or (2) tablet, and even without possessing such a device, the EHR can be accessed via (3) the patient's electronic health card and a PIN. Using one of these three access methods ensures the availability of all existing documents when visiting a healthcare facility the patient has not been to before. Patients with private health

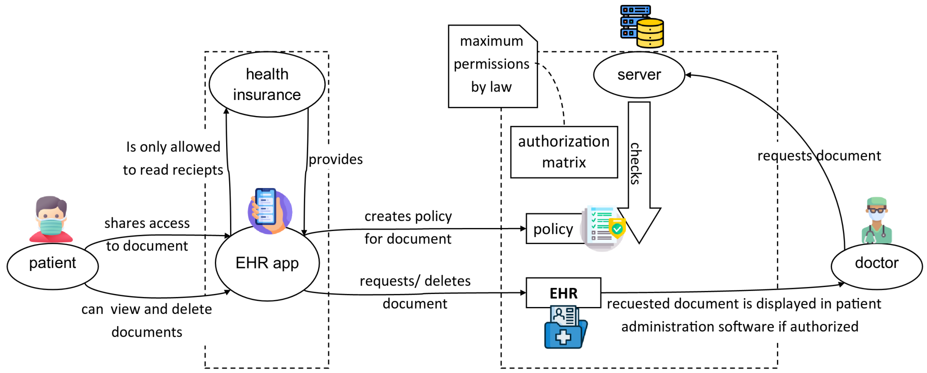

maximum permissions by law
server
health insurance
Is only allowed to read reciepts
provides
authorization matrix
checks
requests document
shares access to document
creates policy for document
policy
patient
EHR app
doctor
requests/ deletes document
EHR
recuested document is displayed in patient administration software if authorized
can view and delete documents

Figure 1: Schematic overview of the German infrastructure.

insurance, without an electronic health card, cannot use the EHR.The patients themselves determine who is granted access to the EHR. The patient defines who may access their data and to what extent it is shown to a specific entity. Further, patients can decide which data is uploaded into the EHR and delete data they do not want anymore.

App Provider: The respective health insurance of the patient functions as the provider of the access app. Thus, there is no central app for all German citizens, but as many apps as there are health insurance companies. However, the health insurance only provides the platform/infrastructure for managing the EHR and does not have access to the data. Some health insurances also provide desktop apps [23]. At the beginning of 2023, there were 85 different apps provided by health insurances [23].

2.2 Mental Models & Privacy

This section first introduces mental models and different investigations in the privacy context.

Mental Models & Investigations. Mental models are internal representations in the human mind used to explain the real world to decide on how to act [25]. Specifically, in the scope of mental models of technology, two model types are distinguished: (1) functional and (2) structural models [37]. The former (functional models) mean that individuals know how to use technology and its implications, yet detailed knowledge on *how* the technology works is not present. The latter (structural models) means that individuals have a detailed understanding of how technology works. Consequently, humans have more or less accurate and detailed mental models [9,25,26,29]. Misconceptions in mental models might lead users to behaviors that do not represent their actual needs [43].

Many existing studies investigated the mental models of individuals in the scope of cybersecurity in different technological contexts in the scopes such as encryption [28, 48], threat perceptions of PC users [44, 45], decentralized identity wallets [27], adversarial machine learning [7]. All studies highlight the importance and impact of mental models in (in)secure behavior.

Investigations of Privacy Mental Models. Mental models inform the behavior of users and profoundly contribute to adopting new technologies [2, 26, 41, 49]. Privacy mental models, in particular, have been shown to impact technology usage in the scope of the digitization [3, 4, 10, 14, 15, 17, 19, 46, 47, 50, 51].

Early investigations particularly considered internet usage and responses to threats [26] demonstrating that individuals with a better technological understanding perceive more risks, but do not necessarily take better precautions compared to individuals with a lower understanding.

Many investigations of IoT settings and smart homes in particular, showed that privacy concerns can form usage barriers that hinder people [2, 41, 49]. The specific concerns are rooted in the physical security of households or hackers gaining access to IoT devices [50, 53] calling out the need for the awareness of data collection, especially when data is sent through the internet [19, 24, 33, 35].

2.3 Investigations of Digital Health Records

Several researchers investigated perceptions of patients and healthcare providers regarding EHRs and PEHRs. In terms of methods, either conversation-based interviews (cf. [30, 31]), card-sorting exercises (cf. [13]), and online surveys [5] were predominantly used to investigate the patient's attitudes towards EHRs. Not surprisingly, patients consider ease-of-use as a dominant factor in adopting (P)EHRs [5, 34, 38].

The literature produced mixed results regarding privacy perceptions which might be linked to cultural differences. Privacy was frequently considered an important topic in the context of digital health in general [34]. When asked for specific concerns, study participants mentioned unauthorized access, e.g., in case PEHR data volumes get lost [30], misuse of the data stored in EHRs, e.g., exposing individuals with stigmatized diseases [31], or increased health insurance contributions for patients with treatment-intensive health conditions [22, 31]. This was shown in the countries Australia (EHR) [30], Canada (PEHR) [5, 22]. These findings related to health insurance perceptions further motivate our investigation because in Germany the health insurances serve as providers for the access apps, yet, should not be able to access all data. Privacy concerns were expressed in the context of hacking attacks [6], since hackers might attack EHRs to gain sensitive information which are concerns similar to those expressed in the context of IoT devices [50, 53]. American studies [13] showed that American patients want to have granular privacy control over how their health data is shared []. However, Swedish patients perceived that health care professionals having access to their EHR would be in the patients best interest and strict access guidelines instead of access control would be a sufficient security measure [30].

Further investigations, however, showed the opposite meaning that individuals might not have privacy concerns because they highly trust the central infrastructure and the Hippocratic Oath from doctors [30]. This was shown for Sweden [30] and Canada where patients stated to adopt the PHR based on trust in the PHR platform [5]. Finally, while Canadian patients were open for using the PEHR [5, 22], they were not aware of the PEHR already existing and being available [22]. The same was observed for Swedish patients [30].

Overall, this shows that different countries and cultures need to be investigated individually because privacy perceptions – much as the concept of privacy in itself – are highly individual.

2.4 Summary

There are many ways to realize EHRs. Germany uses a national infrastructure where health insurances serve as app providers. Yet, related work repeatedly showed that patients have different privacy concerns involving data access of health insurance companies. This paper investigates patient perceptions of this unique infrastructure by capturing mental models through drawing. This adds a new perspective to the literature because conversation-based interviews or surveys were predominantly used.

3 Method

To understand German citizens' existing mental models regarding EHRs, we conducted 21 semi-structured interviews. The interviews consisted of five parts as detailed below. One was a drawing exercise asking participants to sketch their expectations of the German infrastructure. We recorded all interviews with a microphone and a camera and took pictures of the drawings (cf. Appendix A.1 for the complete interview guide). On average each interview took 30 minutes, and participants were compensated with 10€ Amazon vouchers.

Table 1: Demographics of the sample.

ID	Age	Gender	Occupation	Highest Education
P1	18	m	School Student	Still at High School
P2	18	n/a	School Student	Still at High School
P3	18	f	School Student	Still at High School
P4	67	m	Retired	University
P5	26	w	Student	University
P6	27	m	Student	High School Diploma
P7	22	m	Student	High School Diploma
P8	27	f	n/a	University
P9	57	f	n/a	Apprenticeship
P10	23	m	n/a	Apprenticeship
P11	84	f	Retired Accountant	Apprenticeship
P12	89	f	Retired Pharmacist	University
P13	27	f	Physical Therapist	University
P14	54	f	Teacher	University
P15	52	f	Teacher	High School Diploma
P16	18	m	School Student	Still at High School
P17	53	f	Teacher	Apprenticeship
P18	55	m	Manager	University
P19	32	m	Engineer	University
P20	49	m	Firefighter	High School Diploma (FH)
P21	48	f	Sports Therapist	University

Participants & Recruitment. We recruited 21 participants by advertising through mailing lists, social networks, and word-of-mouth. All participants needed to be at least 18 years old. Further, they had to reside in Germany and currently actively use the German health care system by having at least a family doctor. Nine participants identified as male, eleven as female, and one preferred not to say[1]. The average age of the participants was 41.41 years ($min = 18$, $max = 89$, $SD = 21.82$).

The participants had diverse backgrounds with six being students at school or university. Three were retired. Four participants had a finished apprenticeship as highest education, nine had a university degree, four had a high school diploma and four were still in high school. Table 1 provides a detailed overview. All interviews were conducted in German.

Affinity for technology was assessed by the ATI scale which ranges from 1 to 6 [20]. Our sample had an average ATI score of 3.48 ($min = 2$, $max = 4$, $SD = 0.68$).

Study Procedure. The procedure of the semi-structured interviews was as follows:

1) Welcome & Consent: Before the interview, participants were informed about their rights, the captured data, and that they can abort the study at any time without negative consequences. They were further informed that the interview was audio-recorded and transcribed before analysis and that the drawing exercise was filmed without capturing their

[1] There were further answer options (i.e. prefer to self-describe, and diverse). Still, none of the participants chose them.

faces. This and further information were given to them on a participant information sheet that included a consent form that participants were asked to read and sign. Questions by participants were answered during this process.

2) Warm-Up: At the beginning of each interview, participants were asked questions about how their family doctor stores their patient data. Next, we asked about their knowledge and usage of the digital patient file. Afterward, they were given a printed information text on the *general idea* of EHRs in German, meaning that EHRs are stored electronically. Details of the infrastructure were not included in this part to not bias participants.

3) Drawing Exercise – Expectations: Based on the general information text participants read, they were asked to draw a model of the EHR based on their personal expectations. To make it easier for them to get started, they were handed prepared entity pictograms (i.e., doctor, health insurance, patient, generic server, generic devices, and patient file) as well as distractor pictograms next to a sheet of DIN-A4 paper and pencils in various colors as recommended by related work [33, 52]. Further, they were instructed to draw their model in the following scenario to make it easier for them: a doctor wants to access an existing EHR because this doctor is visited for the first time. To get a better understanding of the drawn models, participants were asked to think aloud [8] while drawing such that we could understand their thinking process. When asked to explain their thoughts on how entities are connected, some participants drew arrows. Additionally, they were asked follow-up questions after finishing their drawing to ensure all drawn parts were explained in detail.

4) Infrastructure Perceptions: To round off the interviews, the interviewees were then shown the real model of the German EHR infrastructure as seen in Fig. 1. The infrastructure was explained to them using the scenario of visiting a new doctor as detailed above. After the interviewer has made sure that the interviewee understood the model, the interviewee was asked follow-up questions specifically considering their perceptions of the real infrastructure. The interview was concluded by asking participants about ideas for improving infrastructure and whether this would change the interviewee's willingness to use EHRs. Before the interview ended, participants were given a chance to add any further comments or statements.

5) Demographics & Compensation: The recording then ended and participants were handed a tablet to answer a demographics questionnaire. As the last step, participants were compensated by an Amazon voucher with a value of 10€ (roughly 10 US dollars).

Data Analysis. Before the analysis, we first anonymized all captured data. Audio transcripts were transcribed into written form. To ensure participant identification is not possible by their handwriting in their drawn models, their writing was concealed by machine text. Next, two researchers independently analyzed the properties of the sketches by listing entities chosen and drawn by the participants, the purpose of the entity, and its communications. The researchers compared their lists and resolved disagreements in a meeting. Next, it was analyzed whether participants had functional or structural mental models [37]. For this, the transcripts were also considered to make sure that there are no misunderstandings.

The transcripts were also analyzed by thematic analysis [11]. In the first round, we conducted open coding by assigning codes to meaningful and relevant concepts focusing on our research questions. One researcher who was familiarized with the data generated an initial codebook. The codebook was then verified by a second researcher who was present during some of the interviewers and also had familiarized themself with the transcripts.

This codebook comprised 16 codes (see Table 2 in Appendix B). Following the methodology guidelines for conducting thematic analysis [11], one researcher applied the codebook to all statements. This was then verified by the second researcher and disagreements were resolved. Please note that guidelines for thematic analysis advise against double or multiple independent codings and using the inter-rater reliability to prove reliability [12, p.278-279]. This is because qualitative research acknowledges the influence of the researcher on the process [12]. Finally, four themes emerged from our analysis: (1) the role of health insurance companies, (2) the role of patients, (3) perceived risks, and (4) knowledge gaps and misconceptions.

Ethical Considerations. We took several precautions to protect the identities of our participants. Audio recordings were anonymized and transcribed before analysis. The participants' handwriting in the sketches was concealed by machine text. The consent form had detailed information about the data captured in the study, and the participants' rights and was compliant with the GDPR and national data protection laws. The consent form further mentioned that the study could be aborted without any negative consequences.

Since the study does neither have any risks beyond normal every day nor cause psychological harm, our institutions did not require formal IRB or ERB approval for the kind of study that we did. However, as stated above, we adhered to the strict (inter)national data protection laws and followed best practices for research conduct and transparency.

Limitations. Like most qualitative and exploratory investigations, our study is subject to several limitations that must be considered when reading our results.

First, our study is based on self-reported data, which might be biased due to social desirability, availability bias, and wrong recalls or self-assessments. Consequently, our data only reflects the highly subjective views of our participants. Further, none of the participants had experience with using the German EHRs, hence their assessments are based on their expectations and might be different in case they actively use the EHRs. Yet, we wanted to capture patients' intuitive expectations of this new infrastructure since this also contributes to adoption. Still, especially in evaluating mental models, different subjective models of a concept like the digital health record are beneficial for research on how to counteract respective misconceptions or knowledge gaps. Having comparable experiences is quite challenging due to the high number of health insurance companies and the respective high number of EHR apps. Nevertheless, future work should investigate the actual usage of German EHRs.

Second, while we tried to recruit a diverse sample, our sample might not be representative of the entire German population. Still, our exploratory investigation served as a first step to investigating mental models of the Germans EHR infrastructure. Future work should investigate a representative sample.

Third, our investigation considers the specific use case of Germany and the German infrastructure. Based on that, our results regarding the perceptions are limited to the German system. However, the perceptions of the participants regarding the specific infrastructure can be used to inform the design of other infrastructures as well.

4 Results

The section details the results of the interview study and the drawing exercise. We first describe the sketches of the expected infrastructure. Next, we detail the results from the thematic analysis theme by theme. Whenever meaningful, we provide quotes from the participants that were translated from German. We further provide quantities of mentions to give the reader an impression of how often a specific aspect came up during the semi-structured interviews. However, this should not be mistaken as an attempt to quantify our results. RQ1 is answered in 4.1, 4.2, and 4.3. RQ2 is answered in 4.4, and RQ3 is answered in 4.5.

4.1 RQ1 - Overview of the Sketches

The sophistication of the participants' sketches was quite diverse. Fig. 2 provides some examples. None of the models intuitively described the German infrastructure correctly.

Functional vs Structural Models. Out of the 21 participants, only five participants (P4, P5, P7, P16, P18) had a structural mental model of the EHR which however had several parts that do not correspond to reality. The functional mental models were as their definition says quite simplistic. Most of them just listed a few entities with arrows between them. Some participants with functional models actively voiced knowledge gaps (see Sec. 4.4). A few with structural models (e.g., P5 in Fig. 2b) explained in detail how the data exchange and data management work in their understanding.

Entities. Intuitively, participants chose different entities to be part of their mental model. All participants included patients, doctors, and a central server. Most participants included the health insurance company in their sketches. However, all participants verbally mentioned that health insurance has a role in the infrastructure. Few participants also included other healthcare providers, such as emergency doctors or pharmacists because their access is needed in certain situations. Many participants integrated a smartphone to have data access. Two participants integrated a *"national authority"* (P3, P19). For a full overview of all entities drawn by individual participants, the reader is referred to Table 3 in Appendix C. This table also included access rights and data storage locations.

Similar results were found regarding mental models of decentralized identity wallets, where participants also considered different entities as part of their mental models, and reflected on the trustworthiness of these entities [27].

Storage Location. The participants sketched and mentioned several locations when it came where the EHRs are stored. Most participants mentioned *"a central server"* hosted by authorities, sample comments mentioning the central server are:

- P7: *"I want it [the EHRs] to be managed by a public authority, that would be my dream, like the public health authorities."*

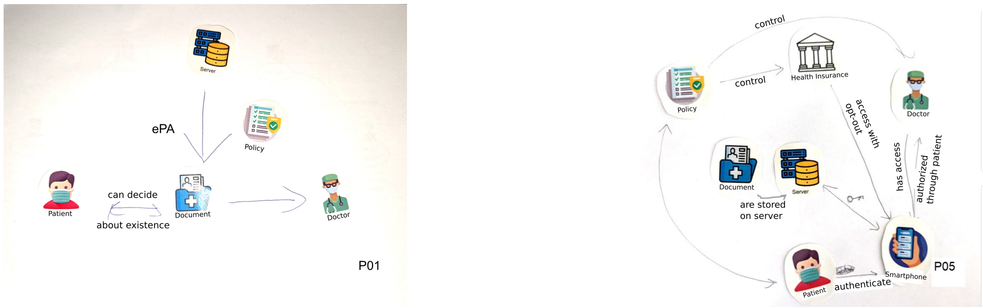
Further participants considered the *"health insurances"* (P8, P11, P16) to host the EHRs, e.g.:

- P11: *"The server is hosted by the health insurances because those should be trustworthy."*
- P8: *"By the health insurance, or somewhere else, I don't know where exactly."*

Two participants (P12, P14) considered the doctors to store the EHRs, while some participants considered several storage locations, instead of one, such as *"on a chip card[2] and a server"* (P18), or *"on a mobile device, the patient card, a server and with the health insurance"* (P6).

Access. Data access was an essential topic in most interviews. Considering the expected data access, the first group of participants expressed an *unspecified* access to EHRs by different entities like *"health insurances"* ($N = 5$), *"patients"* ($N = 4$), and *"doctors"* ($N = 3$). Some participants also mentioned *"hospitals"* ($N = 1$), *"pharmacists"* ($N = 1$) and

[2] By this, they mean the German health care chip card that each member of a statutory health insurance has.



(a) Functional Mental Model P1

(b) Structural Mental Model P5

Figure 2: Participants' sketches showing examples of their mental models. We replaced participants' handwriting with digital labels to enhance readability, and provide participant anonymity and for translation purposes.

individuals close to the patient, such as *"family members"* ($N = 1$) and those with access when the *"patient gave consent"* ($N = 1$). Yet, most participants expected doctors only to have access if the *"patient grants it"* ($N = 12$).

When asked about specific access rights, the patients considered different entities to have *complete read and write access* to their EHRs, namely health insurance companies ($N = 2$) and patients ($N = 4$). There were also various expectations towards doctors ($N = 4$), doctors in charge of the patient ($N = 1$), and doctors in emergency situations ($N = 1$).

Participants expressed various entities to have *complete read access* only to their EHRs, particularly health insurance companies ($N = 3$) and patients ($N = 1$).

Access Control. This brings us also to the topic of access control rights. Here participants had several ideas on who is managing access control to their EHRs.

Most participants considered the patients to be somehow involved in controlling access rights, such as:

P7: *"The best way, at least the way I hope, is that the patient first has to confirm somehow that he [the doctor] is allowed to do that [access the EHR]."*

P14: *"And [the doctor] should only have access to the server via the patient. So if the patient says, 'yes, okay' then the doctor can access it."*

Among them, some participants made a connection to existing granting of permissions in the medical context required by the GDPR, such as:

P8: *"I have to sign such documents all the time and consent that my data is shared. Because of that, I added that to my model out of habit."*

Yet, some participants also considered doctors and health insurance companies to have access control rights.

P11: *"Basically, I would say the family doctor. That's the one, right? But if he should give me the documents for the next doctor, he practically hands that over, does he? [...] In principle, the health insurance company is probably the highest, which also has a little bit of control over it."*

P16: *"And if one is then with the physician and the physician asks, 'I need or I would like to have access to provide treatment', then the physician can put a request to it, which must be confirmed by the patient and by the health insurance."*

Similar to our results access control played an important role in the mental models of decentralized identity wallets [27].

Delete. One participant (P19) mentioned that patients should be allowed to delete records.

4.2 RQ1 - Theme 1: The Role of Health Insurance Companies

The first theme identified in our analysis considers the specific role of health insurance companies within the infrastructure of EHRs specifically considering privacy and trust aspects.

Privacy towards Health Insurances. A slight majority of participants considered privacy towards health insurance as essential. Particularly, they were concerned that by having access to detailed patient data, health insurance companies might increase the contributions of patients with certain diseases or risks. Sample comments are:

P17: *"The health insurance and access to the data, I think that's kind of pretty difficult. [...] You might be categorized differently in terms of contributions, so at least when you apply for health insurance, I think that's very, very tricky if they had access to [the EHRs]."*

P18: *"The health insurance company needs no information at all, except about what is needed for billing. That's all they really need. It's nice when the health insurance company cannot access the content. In the best case, the information that the health insurance company needs* *is sent to them from the server. That's how it would be desirable from my point of view."*

These results confirm concerns regarding the contributions to the health insurance companies from related work that investigated Australia [30] and Canada [5, 22].

Health Insurances as Trust Anchors and Backup. The remainder of the participants, however, voiced opposite opinions, specifically considering the health insurance companies as a trusted entity that also observes whether health care providers, such as doctors act genuinely:

P5: *"Access for the health insurance would probably be good, if that is somehow regulated in such a way that the health insurance automatically, if that is officially your health insurance, also always has access to your file, because I can imagine that for emergencies, if you yourself somehow don't have the possibility to authorize it, it's kind of stupid if your health insurance doesn't have access to it, besides, it feels like it has access to all things anyway, right?"*

P16: *"The server is provided by the health insurance because people trust it or at least it should be trustworthy."*

Trust playing a role in mental models was also observed in comparable studies [27].

Health Insurances as App Providers. As evidenced by the privacy issues regarding health insurance companies and the opposite opinions regarding trust anchors, it is challenging to provide a solution that fits the needs of all individuals. Some participants also commented on the health insurance companies as app providers. The first group considered this to be a negative aspect:

P19: *"If health insurances have access, they could change the contributions for each individual. I don't trust that all health insurance companies will be completely trustworthy 100% of the time. I don't trust that they wouldn't try to get some kind of benefit through the app provided by them."*

Several participants even suggested that the app provider should not be the health insurance companies:

P16: *"There should be a law, which describes the all guidelines exactly. Yet, health insurance companies might maybe find some loophole, you never know. So it's not that I suspect that they will do that [...] I trust the state more than the health insurance companies, which are still an institution somewhere, which also have to earn money."*

P20: *"Of course [the health insurance] needs some access. That is convenient, but I don't think that it should be involved in providing the app. I think that is very critical."*

P17: *"The health insurance company is only allowed to see prescriptions. I find that somehow strange that they then provide the app."*

4.3 RQ1 - Theme 2: The Role of Patients

The second theme revolves around the role of the patients within EHR infrastructures.

Control by Patients. First, participants expressed to have a variety of benefits of using the German EHRs specifically focused on the control exerted by patients:

P5: *"I really like that the patients can authorize doctors. They can also use the app to revoke that."*

P7: *"And then I can simply change policies by the app? That's really awesome."*

However, since patients using the EHR have quite a lot of responsibility, this might result in problems, because patients could be overwhelmed:

P8: *"On the other hand, it could also be too much for people who do not have an overview of what could be important or not. Where it is then perhaps easier to have all the findings and then can if they are generally not so familiar with digital media."*

P14: *"That is way too complicated for – and I'm not even careless – but there are people who think about it even less than I do, I think. So, it is much too complicated. In the end, the patient probably can do everything."*

Data Deletion by Patients. Patients are allowed to delete data from their EHRs. Some participants expressed concerns in connection with that, specifically fearing that people might "mindlessly" delete data that might, later on, be important or otherwise negative impacts on patient care:

P21: *"It might happen that important things are deleted, I mean information that is important for the doctor."*

P13: *"I just don't know whether it should be possible to delete these things as a patient, which I see a bit critically. I think it is important to archive such sensitive data."*

This risk is also reflected in official documentation provided to healthcare professionals specifically instructing them to make sure to have the data also locally stored at their practice [21].

Further participants feared that patients maliciously manipulate their files to gain a benefit:

P12: *"And that can't be right. There are professions where you need a health certificate. I needed one of those, for example. And if there are things in your patient file that contradict that, then you simply delete them. And apply for a job with a deleted patient file. That can't be good."*

P3: *"Patients should not delete information, they could repeatedly have prescriptions for prescription drugs written for them."*

However, data deletion by patients was not completely perceived in a negative way. Two participants liked that patients have the right to delete their data:

P16: *"Otherwise, I think it's good that the patient has so much control over the document. Because they have all the information, they can say whether they want the doctor to see the document, and then they can delete it if they no longer want to have it. I think that's good."*

P20: *"If something not needed is registered, then, of course, it will be deleted. This does not contribute to finding the truth about someone who is lying unconscious somewhere."*

4.4 RQ2 - Theme 3: Gaps & Misconceptions

As already stated above, the intuitive expectations of the infrastructure often did not match reality. Below, we detail knowledge gaps and misconception expressed by participants.

EHRs in Germany Are Not Available. None of our participants did use the EHR, although it was introduced in January 2021, which is more than one year before our study. The vast majority of them have not even heard about it. Here, several participants struggled to believe that the EHR is indeed available in Germany, leading to interesting conversations with the experimenter:

P20: *"I really like the idea and would welcome its introduction."*

P18: (after experimenter tells that the EHR is available for all patients in Germany) *"I just don't believe it."*

How Does Authentication & Authorization Work. Participants directly expressed several knowledge gaps they were aware of. This was in the context of authentication and authorization where participants struggled to explain how such a procedure might be done ...

P5: *"I know so little about it [health records], I don't know, for example, whether, well, because that must be password-protected somehow, or otherwise protected. [draws] I just noticed that I have a knowledge gap because I don't know where or how one could authorize the doctor."*

... but also in the context of consent, where participants expressed difficulty to explain when their consent is needed and when not, e.g.:

P9: *"That's kind of a big question mark for me because I don't know, I mean I know that somewhere there are agreements, a declaration of consent is made, also that others are allowed to access it. What exactly the guidelines are, I don't know."*

Doctors Have Full Control. Participants had various ideas on how doctors are involved in access control as mentioned above. In particular, doctors were given more power and more authority compared to reality:

P11: *"Basically, I would say right from the start, the GP [controls it]. But if he could give me the documents for the next doctor, he practically hands them over."*

P4: *"Patient don't have access to it. They just have to sign a consent form."*

One participant even said that doctors – once authorized – can also view the data offline:

P6: *"I mean, even if it [the health record] is not online, the doctor can still see the data if he wants to. That's why I would say that the doctor always has to sign a declaration of consent confirming that everything remains anonymous and is not passed on to third parties, that's what I would say. He can always call up the data."*

Emergency Access is Available. Two participants explicitly mentioned that emergency doctors have access to their data in case they are unconscious. However, the data can only be accessed in cooperation with the patients:

P4: *"If I have an accident, it would make sense if I wouldn't have to give them [the emergency doctors] any access authorization at all, but that they have access to my medical records via a special access right, so that they can act immediately."*

P7: *"So it would be cool if an emergency doctor could do that, for example, if they somehow arrive at an emergency scene or something and can then call up something in that direction. That would certainly be very practical."*

App Control is Impossible. When explained that the access control is done via an app or physically via the health insurance card, some participants still struggled with this:

P12: *"Using an app [to grant access], but the patient can't do that. What sense does that make? Nobody can grant access rights through a smartphone. No one is allowed to do that."*

Health Insurance Have All-Access. Most misconceptions expressed by participants were in connection to health insurance companies. Several participants thought that the health insurance has full access to their EHRs because this is needed for billing:

P11: *"In principle, the health insurance is the highest entity which also exerts most control."*

P12: *"The health insurance must be involved [in storing and managing the EHRs]. They have access to the data anyway through the prescriptions from the doctors."*

This seems to be related to a general misconception about the data that German health insurance companies can access that is already present with analogue patient records. As stated in Sec. 2.1 health insurances do not have access to patient records. Perhaps interestingly, here misconceptions from the analog world diffused into the digital world.

Similar to the privacy aspects of health insurance companies, some patients saw full access as a requirement for health insurance companies to calculate their contributions:

> P2: *"The health insurance companies also because they often want to know what kind of illness people have or whether people have any illnesses to somehow set the contributions accordingly or so that they can adjust to what will happen in the future."*

4.5 RQ3 – Theme 4: Perceived Risks

Besides the risks associated with the roles of the insurance companies and patients, participants perceived further risks based on the central storage of the EHRs and third parties.

Centralized Storage. Some participants considered the central storage of the German infrastructure to be problematic in the context of security:

> P3: *"Therefore, my problem is not the handling with [the data], but rather that it is only stored in one place and that this is, so to speak, probably then quite or much easier to attack than paper files."*

Based on that, participants had various expectations and suggestions in the context of security, such as *"using encryption"* (P5) or *"something similar to two-factor authentication"* (P19), or *"letting doctors only access EHRs of patients who are physically present"* (P19).

Further, participants wanted that doctors have additional local files, such that too sensitive information does not get uploaded to a central entity:

> P14: *"Overall, I like the idea of a general server, but I think that he [the doctor] should have a private file. Private, to store sensitive data. I don't want that everything I'm telling my doctor ends up on a server. No way!"*

Third Parties. Participants expressed that there might be further privacy risks if third parties, such as hospital providers, commercial operators, or the employer get access to the data:

> P18: *"But these are also some purely commercially operated hospitals, and of course, you can't trust them, I say."*
>
> P14: *"The health insurance company is a problem because if they know too much about a patient, which is already the case today, they may not accept him or her. Who knows what prejudices they may have? And also, I would like to say again here, the working world, employers, and so on, they should not be allowed to know everything either."*

Participants further praised that information about them might become more easily available when needed:

> P14: *"Of course, I think it's great when I imagine I have an accident and then my name is entered and then everything that has been stored so far appears. And from this information, be it just my blood group, my life could be saved. I think that's great."*
>
> P1: *"So I mean, you can perhaps also determine diseases that are perhaps somehow related, also sooner as a doctor alone."*

Finally, some participants liked they do not need to bring any existing doctor's letters or other kinds of documents with them and that burden is taken away from them:

> P18: *"An advantage is that the patient does not have to bring anything."*
>
> P5: *"I'm also like that, I tend to lose documents and then need to look for them forever. And I imagine that it's very practical to have them somehow online."*

Missing Assurance. Similar to other existing studies about data sharing in different domains [19, 24, 35], we found that participants want options for (a) consent sharing and (b) assurance about the status of their EHR:

> P18: *"At the moment, the patient basically has hardly any control options. He can look at these documents and delete them, but he doesn't know whether the server always shows all the documents. [...] He probably has, I don't know, any knowledge about what is stored on the server and who has looked at it or so, so he is only at the end and he gets access to his data via an app. But who says that the data is displayed in full or that it then becomes transparent?"*

5 Discussion

In this paper, we explored the mental models of German EHRs, which is a national infrastructure that stores the health data of all German citizens wishing to use it. In the remainder, we discuss the management options of the German EHR by app and health card, perceptions of the role of health insurance companies, data manipulation, the involvement of patients, and their privacy implications. We further provide key takeaways and recommendations for digital infrastructure providers, e.g., developers and system designers, and healthcare providers. Finally, we compare our findings with results of similar studies conducted in other countries.

App- & Card-based Management. Patients can use an app from their health insurance company or an electronic health card to authorize access to documents in their EHR. While the electronic health card is an easy and existing way to authorize data access, it also comes with many limitations. Patients must be physically present at the doctor's office to manage their documents. Since doctor visits are already quite limited in terms of duration, it is questionable whether doctors would indeed take more time to allow patients to browse and manage their data. While having card-based access is a possible fallback mechanism, it is unrealistic for actual usage.

Within the context of other IT systems in Germany, having such an app is quite a unique aspect. No participant initially thought that access is controlled this way. Having health insurance companies as app providers results in tension because (a) the companies only should have access to data needed for billing purposes, yet (b) the app allows patients also to add or delete documents. Consequently, patients need to trust that health insurance companies do not access this data.

The decentralized infrastructure was criticized by our participants for several reasons: trust assumptions are made towards health insurance companies, and there might be impacts on convenience or ease of use. Further, certain groups of individuals are excluded, development and maintenance come with challenges, and the apps create attack vectors. Finally, the current infrastructure did not match the participants' mental models which in turn might result in a low adoption as also shown in related domains, such as encryption [28, 48].

> 💡 **Takeaway 1: Challenges for Chip Card Users**
>
> Patients with the electronic health card only get a very limited service and are dependent on their doctors to exert control over their EHR.
>
> **Recommendation 1:** The government should offer different possibilities for EHR access (e.g., smartphone & desktop apps, options for people without technical devices like kiosks). Patients should not depend on any healthcare provider to manage their EHRs.

Perceptions on Role of the Health Insurance Company. While most participants expressed concerns that insurance companies might use EHRs as part of their business model, some participants considered them to be a trusted supervisory authority that ensures the doctors do not break policies.

To dive into this more deeply, we need to understand the details about the German health insurance system given in Sec. 2.1. Further, we have to note that patients with statutory insurance always get the electronic health card which is needed to use EHRs. Private patients rarely get such a card meaning that the EHR is for patients with statutory insurance.

As stated above, private insurance companies rely on preexisting conditions when making the decision to insure an individual or calculate contributions[3]. Consequently, it is already part of the business model. Current contribution models are not dynamic because private health insurance companies are only allowed to increase contributions if they can prove that the overall costs are rising. Hence, it is not allowed to consider new conditions. Since private insurance companies currently are not part of the EHR, private patients do not have to fear consequences like changing contributions. Further, it is not allowed by law. However, the benefits of EHRs should also be available to patients with private health insurance, and the infrastructure should consider that.

Health insurance companies need certain information about patients to deliver their service as rightfully assumed by our study participants. Yet, the information the statutory insurances receive is limited to that needed for the billing process [39]. The German infrastructure models this process, yet participants particularly struggled that health insurances provide the app to serve as a data controller. When installing the app, consent forms might ask patients to consent to share more data with health insurance companies than needed. Considering that most participants had a wrong mental model here, it might be easy for a health insurance company to get consent from their clients. Further, health insurances in Germany also have optional bonus programs rewarding patients for specific actions, e.g., yearly check-ups or being a sports club member. Currently, insurance apps promote these programs allowing them to combine even more data.

Besides the results from our study, this results in more problems: first, patients no longer having German health insurance might lose access to their EHRs which is difficult from the GDPR perspective. Second, the landscape of different apps is fragmented since 85 insurances offer EHR apps which also defeats the cost reduction efforts of EHRs. Third, the development, maintenance, and test process for the apps is challenging because patients might have issues with data that the health insurance is either legally not allowed to be seen or the patient does not want to share it, and fourth, as stated above individuals that do not want to or cannot use an app have challenges to overcome in case they wish to exert control over their data.

For the reasons above and a better alignment with patient expectations, there should be a central infrastructure. Access software, such as apps, should be provided by an independent provider, e.g., the one that also provides the server. Further, API documentation should be published in case individuals wish to use their own system to access their EHR. For this, a central access control system is needed that allows authenticating patients to prevent data leakage to others.

> 💡 **Takeaway 2: Insurances Should Not Provide Apps**
>
> Having health insurance companies as app providers is a challenging aspect that raises several concerns because there is tension between their responsibilities as app providers and patient privacy.
>
> **Recommendation 2:** A central access and management option should be provided by an official entity different from the health insurance company.

[3] While it is legally challenging to refuse patients, the monthly contributions can get quite high, so some individuals choose statutory insurance in case of pre-existing conditions.

Data Manipulation. Some participants considered their insurance company a controlling entity that ensures doctors act genuinely. Currently, it is challenging to reveal error-prone data without the knowledge of a healthcare professional. Insurance companies cannot have this function either because of the trust aspects. Further, patients rightfully have a lot of power over their data. While most patients likely act genuinely, there might be cases where patients maliciously manipulate their files. Further, even if patients act genuinely, they might misjudge the importance of the stored data. Official documentation for doctors instructs them to make local copies of documents to ensure their availability. However, doctors are human as well and might forget this. A possible solution for that is allowing patients and healthcare professionals to mark certain records for verification by a trusted third entity that can trigger an investigation in case a record is suspicious.

💡 Takeaway 3: Dispute-Resolution is Needed

Patients and doctors might add or remove data that is useful and needed.
Recommendation 3: Methods for record verification should be provided. Further, if access is granted to doctors, a local copy should be stored automatically.

Patient Involvement. Data access to the German EHR without patients is impossible. This gives patients the ultimate power over their data which was requested by patients studied in other countries [13]. Yet, as also commented by our participants, in health care, there might be situations where the patient is not available, but data access is critical, for instance, in case of an accident. Currently, there is no way for doctors to access the EHR. Similar to other scenarios with fallback access, there might be a scratch field on the patient's electronic health card that allows data access. A scratch field is a hidden field on the electronic health card similar to a scratch card. In an emergency, doctors could access the EHR by physically uncovering credentials under the scratch field to ensure the best possible patient treatment. Patient could see that someone uncovered the credentials, since removing a scratch field is irreversible.

💡 Takeaway 4: Provide Emergency Access

The ultimate power of patients limits data access in an emergency situation.
Recommendation 4: Provide a secure and easy-to-use way for emergency data access.

German Perceptions vs Other Countries. This section compares our results to related studies conducted with Canadian [5, 22], American [13], and Swedish [30] patients.

Similar to our participants, for Canadian patients the biggest motivator for adopting PHRs is having access to their own medical data, and perceiving the PHR as useful in terms of usability, functionality and accessibility [5]. This is reflected in our findings by participants liking the extend of control patients have over their EHR and also confirms the findings of the American studies [13]. Our participants perceived the necessity of trusting health insurance companies as critical, since they function as providers of the different German EHR applications. This contrasts results from Canada [5].

Perhaps interestingly, since EHRs are quite new, Canadian [22] and Swedish participants were not aware of their digital infrastructure similar to our participants [30]. This implies that right now participants do not use the EHR. Resulting in their mental models not having impact on their behavior. Since we evaluated some of their misconceptions, future research can develop measures to counteract those and therefore get patients to use the EHR.

The similarities in our results we found compared to studies from other countries, show that our four takeaways based on patients mental models of the German EHR can also be applied in a broader context. However, we would like to add that the specific cultural context also should be carefully considered when designing EHR infrastructures.

6 Conclusion & Future Work

This paper investigated mental models of electronic health records (EHRs) of German citizens in the context of introducing nationwide centralized EHRs. In this investigation, we focused on aspects related to data sharing, privacy, access management, and trust. We interviewed 21 individuals that currently reside in Germany and use the German health system. Using semi-structured interviews and a drawing exercise, we captured the mental models of patients identifying four core themes.Mostly, participants had incorrect ideas regarding the role of health insurance companies. In Germany, they can only access the data needed for billing purposes, yet participants thought that health insurances have all access, manage the EHRs, or even act as a trusted authority. In the German EHR system, health insurances serve as app providers. The apps can be used by patients for policy management of their EHR. This results in tension between the insurance company as an app provider and the fact that they only have limited data access. Further, patients in Germany are allowed to add and delete EHR documents. This was critically questioned by many participants who feared a negative impact on diagnoses.

Based on our investigation, we provide valuable insights in the form of recommendations for digital infrastructure providers, such as developers, system designers, and healthcare providers. Future work should specifically investigate possibilities for dispute resolution, e.g., in case a patient or doctor adds non-credible data. Further, mental models of other types of infrastructures should be captured and compared with the German ones.

Acknowledgements

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. It was furthermore supported by the German Federal Ministry of Education and Research (BMBF) in the project "Verbundprojekt: Digitale Fitness für Bürgerinnen und Bürger – realistische Risikowahrnehmung, sichere Routinen - DigiFit" ("Joint project: digital fitness for citizens - realistic risk perception, secure routines - DigiFit") – grant number 16KIS1646K.

References

[1] Drei viertel der deutschen wollen elektronische patientenakte nutzen. *Bitkom e.V.*, Mo., 06.12.2021 - 10:10.

[2] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '19, pages 1–16, Berkeley, CA, USA, 2019. USENIX Association.

[3] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Understanding physical safety, security, and privacy concerns of people with visual impairments. *IEEE Internet Computing*, 21(3):56–63, May/June 2017.

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):59, 2018.

[5] Norm Archer and Mihail Cocosila. Canadian patient perceptions of electronic personal health records: An empirical investigation. *Communications of the Association for Information Systems*, 34(1):20, 2014.

[6] Sahil Bhagat, D Fontaine, and K Gibson. Danish healthcare information technology-an analytical study of consumer issues. *Worcester, MA: Worcester Polytechnic Institute*, 2010.

[7] Lukas Bieringer, Kathrin Grosse, Michael Backes, Battista Biggio, and Katharina Krombholz. Industrial practitioners' mental models of adversarial machine learning. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 97–116. Usenix Association, 2022.

[8] Ted Boren and Judith Ramey. Thinking aloud: Reconciling theory and practice. *IEEE transactions on professional communication*, 43(3):261–278, 2000.

[9] Christine L. Borgman. The user's mental model of an information retrieval system: An experiment on a prototype online catalog. *International Journal of Man-Machine Studies*, 24(1):47–64, 1986.

[10] Denys Brand, Florence D. DiGennaro Reed, Mariah D. Morley, Tyler G. Erath, and Matthew D. Novak. A survey assessing privacy concerns of smart-home services provided to individuals with disabilities. *Behavior Analysis in Practice*, 13:11–21, 2019.

[11] Virginia Braun and Victoria Clarke. Thematic analysis. 2012.

[12] Virginia Braun and Victoria Clarke. *Successful qualitative research: A practical guide for beginners*. SAGE Publications, London, 2013.

[13] Kelly Caine and Rima Hanania. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, 20(1):7–15, 2013.

[14] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the Conference on Ubiquitous Computing*, UbiComp '12, pages 61–70, New York, NY, USA, 2012. ACM.

[15] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. Alexa, can i trust you? *Computer*, 50(9):100–104, 2017.

[16] Donald P Connelly, Young-Taek Park, Jing Du, Nawanan Theera-Ampornpunt, Bradley D Gordon, Barry A Bershow, Raymond A Gensinger Jr, Michael Shrift, Daniel T Routhe, and Stuart M Speedie. The impact of electronic health records on care of heart failure patients in the emergency room. *Journal of the American Medical Informatics Association*, 19(3):334–340, 2012.

[17] Kovila PL Coopamootoo and Thomas Groß. Mental models: an approach to identify privacy concern and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 9–11, 2014.

[18] B Devkota and A Devkota. Electronic health records: advantages of use and barriers to adoption. *Health Renaissance*, 11(3):181–184, 2013.

[19] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '17, pages 399–412, Berkeley, CA, USA, 2017. USENIX Association.

[20] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: Development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human-Computer Interaction*, 35(6):456–467, 2019.

[21] Bundesminsterium für Gesundheit. Die elektronische patientenakte (ePA). https://www.bundesgesundheitsministerium.de/elektronische-patientenakte.html, 2021.

[22] Marie-Pierre Gagnon, Julie Payne-Gagnon, Erik Breton, Jean-Paul Fortin, Lara Khoury, Lisa Dolovich, David Price, David Wiljer, Gillian Bartlett, and Norman Archer. Adoption of electronic personal health records in canada: perceptions of stakeholders. *International journal of health policy and management*, 5(7):425, 2016.

[23] gematik GmbH. Die epa-app die angebote der gesetzlichen krankenkassen. https://www.gematik.de/anwendungen/e-patientenakte/epa-app, last-accessed 13-Feb-2023, 2023.

[24] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. The catch(es) with smart home: Experiences of a living lab field study. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 1620–1633, New York, NY, USA, 2017. ACM.

[25] Philip N. Johnson-Laird. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Number 6. Harvard University Press, Cambridge, MA, USA, 1983.

[26] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '15, pages 39–52, Berkeley, CA, USA, 2015. USENIX Association.

[27] Maina Korir, Simon Parkin, and Paul Dunphy. An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 195–211, Boston, MA, August 2022. USENIX Association.

[28] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263. IEEE, 2019.

[29] Todd Kulesza, Simone Stumpf, Margaret Burnett, Sherry Yang, Irwin Kwan, and Weng-Keen Wong. Too much, too little, or just right? ways explanations impact end users' mental models. In *Proceedings of the IEEE Symposium on Visual Languages and Human Centric Computing*, VL/HCC '13, pages 3–10, Piscataway, NJ, USA, Sep. 2013. IEEE.

[30] Elin C Lehnbom, Andrew J McLachlan, and Jo-anne E Brien. A qualitative study of swedes' opinions about shared electronic health records. In *MEDINFO 2013*, pages 3–7. IOS Press, 2013.

[31] Elin C Lehnbom, Andrew J McLachlan, and E Brien Jo-anne. A qualitative study of australians' opinions about personally controlled electronic health records. In *HIC*, pages 105–110, 2012.

[32] CY Lu and E Roughead. Determinants of patient-reported medication errors: a comparison among seven countries. *International journal of clinical practice*, 65(7):733–740, 2011.

[33] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. Roles matter! understanding differences in the privacy mental models of smart home visitors and residents. In Adalberto L. Simeone, Raf Ramakers, and Cristina Gena, editors, *20th International Conference on Mobile and Ubiquitous Multimedia*, pages 108–122, New York, NY, USA, 2021. ACM.

[34] Neethu Mathai, Tanya McGill, and Danny Toohey. Factors influencing consumer adoption of electronic health records. *Journal of Computer Information Systems*, 62(2):267–277, 2022.

[35] Mateusz Mikusz, Steven Houben, Nigel Davies, Klaus Moessner, and Marc Langheinrich. Raising awareness of iot sensor deployments. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*, London, UK, 2018. IET.

[36] NHS. How to get your medical records. https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-get-your-medical-records/, 2021.

[37] Donald A. Norman. Some observations on mental models. In *Mental Models*, pages 15–22. Psychology Press, 2014.

[38] Jamil Razmak and Charles Bélanger. Using the technology acceptance model to predict patient attitude toward personal health records in regional communities. *Information Technology & People*, 31(2):306–326, 2018.

[39] Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung. Artikel 1 des gesetzes v. 20. dezember 1988, bgbl. i s. 2477, 1988. https://www.gesetze-im-internet.de/sgb_5/.

[40] Stiftung Gesundheitswissen. Die elektronische patientenakte (epa): Wie sie funktioniert und was sie bringt. https://www.stiftung-gesundheitswissen.de/gesundes-leben/e-health-trends/die-elektronische-patientenakte-epa-wie-sie-funktioniert-und-was-sie, 31.01.2023.

[41] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. I don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, SOUPS, Berkeley, CA, USA, 2019. USENIX Association.

[42] Ahmad Tubaishat. The effect of electronic health records on patient safety: A qualitative exploratory study. *Informatics for Health and Social Care*, 44(1):79–91, 2019.

[43] Joe Tullio, Anind K. Dey, Jason Chalecki, and James Fogarty. How it works: A field study of non-technical users interacting with an intelligent system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, page 31–40, New York, NY, USA, 2007. Association for Computing Machinery.

[44] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery.

[45] Rick Wash and Emilee Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, Ottawa, July 2015. USENIX Association.

[46] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Benefits and risks of smart home technologies. *Energy Policy*, 103:72–83, 2017.

[47] Peter Worthy, Ben Matthews, and Stephen Viller. Trust me: Doubts and concerns living with the internet of things. In *Proceedings of the ACM Conference on Designing Interactive Systems*, DIS '16, pages 427–434, New York, NY, USA, 2016. ACM.

[48] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Symposium on Usable Privacy and Security*, pages 395–409. Usenix Association, 2018.

[49] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. ACM.

[50] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security & privacy concerns with smart homes. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '17, pages 65–80, Berkeley, CA, USA, 2017. USENIX Association.

[51] Yu Zhai, Yan Liu, Minghao Yang, Feiyuan Long, and Johanna Virkki. A survey study of the usefulness and concerns about smart home applications from the human perspective. *Open Journal of Social Sciences*, 2(11):119, 2014.

[52] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 'home, smart home'–exploring end users' mental models of smart homes. In *Mensch und Computer 2018-Workshopband*, pages 407–417, Bonn, Germany, 2018. Gesellschaft für Informatik e.V.

[53] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. Assessing users' privacy and security concerns of smart home technologies. *i-com*, 18(3):197–216, 2019.

A Study Materials

A.1 Interview Guide

This section provides the interview script using for the semi-structured interviews.

- **Welcoming & Consent** (not recorded)
  - *Welcome to this interview and thank you very much for participating. The interview will start with an introduction, where you will be asked some general questions about the topic and you will get some information about it. Then, follows a part in which I ask you to draw something here on the paper. Further, I'll ask you some questions about your drawing. At the very end, I'll ask you to fill in a short questionnaire about yourself. There are no right or wrong answers, I'm always interested in your personal opinion.*
  - *Please read this information sheet completely and sign it. If anything is not clear, please ask me.*
  - *Once, you're ready, I'll start the recording and let you know.*
- **Warm-Up** (audio-recorded)
  - *I'm starting the audio recording. Do you agree being recorded?*
  - *To get us started with the topic, I would like know: Do you know how your primary care physician stores your patient data?* (Possible help, if participant struggles: *Does they use paper files or maybe a PC or something else?*
  - *The main topic of today's interview are digital health records (German: elektronische Patientenakte, short: ePA). Have you heard about the digital patient file – short ePA – in Germany?*
    - (If yes:) *Can you briefly describe what it is?*
  - *Have you ever used any kind of digital patient file?*
    - (If yes:) *Do you use it regularly or just once?*
  - The participant gets the following information text about the ePA and is asked to read it: The electronic patient file (ePA) stores all important information on a patient's state of health and medical history. The idea is that data, such as medications taken, previous treatments or the results of imaging procedures are always available when a patient visits a doctor. Unnecessary multiple examinations and duplicate treatments can thus be avoided. Possible interactions between different medications can also be better taken into account in advance. The bundling of health-related information in the ePA is also expected to improve care in general. For example, the maternity passport, the yellow examination booklet for children, and the vaccination record will be available digitally from 2022. The most important medical data will be stored regardless of location and can be accessed from anywhere. The text is taken from official online documentation [40].
  - *Do you have any questions regarding the digital patient file?* (Questions about technical details were postponed to after the interview to not bias participants.)
- **Drawing Exercise** (audio- and video-recorded)
  - *Now, we start with the second part of the interview. Now, I'm interested in your idea, how the ePA works. For this, I'm asking you to make sketch of that using the paper and pens in front of you. We also have a few icons you can optionally use to make drawing easier for you, but this is optional. As explained before the interview, the drawing will be filled but your face cannot be seen. To make it a bit easier for you, we consider the following scenario: Assume a patient visits a new doctor who wishes to access an existing patient record. Do you have any questions regarding that?*
  - *While drawing please think aloud and explain me what you draw and why.* The experimenter asks questions about the entities and data drawn by the participants to get a full understand of the participant's ideas, such as:
    - *What happens with files?*
    - *Where are files stored?*
    - *Who has access to the files?*
    - *Who is allowed to manage the files?*
  - *Thanks for explaining everything to me.*

- **Infrastructure Perceptions** (audio- and video-recorded)
  - The participant is shown and explained the real model of the digital patient file based on Fig. 1:
    In this part of the interview, we take a look at the real German infrastructure using the scenario from before. The doctor requests a document from the ePA from a central server via their patient management system. All patients' ePAs are stored on this central server. There is one authorization database that defines the authorizations for different actors on different types of documents. There is also a policy for each document, on which individual access permissions are defined. Based on these, the server checks the authorization of the request and, if necessary, sends the requested document to the doctor. Patients use a mobile app from their health insurance company to create and edit authorizations for their documents. They can also use the app to view and delete all documents. Hence, the app changes the policy stored on the server accordingly or deletes the documents. Do you have any questions about that?
  - *Would you like to use this infrastructure?*
    - (If yes:) *Why?*
    - (If no:) *Why not?*
  - *Let's look at this infrastructure together. If you could decide yourself about the structure, access control management, etc., is there anything that you would like to change? If so, why? You can also just draw these changes on the paper. How does this influence your willingness to use the ePA?*
  - *Do you have further comments or questions?*
  - *I'm stopping the recording.*
- **Demographics & Compensation** (not recorded): Participants are asked to fill in the demographics questionnaire and the reimbursement form.

B Codebook

This section provides the codebook used to analyze the transcripts.

Table 2: Table displaying the qualitative codebook.

Code	Description	#
data_exchange	Participant explains how and between whom data is exchanged in the participants model	4
disapproval	Participant explains reason to refuse using the EHR	4
data_storage	Where the EHR is stored in the participants model	34
privacy_awareness	The participant wants to explicitly protect specific data	15
expectations	Requirements the participant expects from the infrastructure	22
access_rights_allocation	How access to the EHR is granted to different stakeholders in the participants model	43
terminological_misunderstanding	The participant had a different understanding of a specific term	25
knowledge_gap	The participants claims to not know something	22
editing_ability	Who can change the information in the EHR in the participants model	41
perceived_advantage	The participant perceives a feature of the EHR as an advantage	12
modification_idea	The participants has an idea for improving the real model of the EHR	26
positive_attitude	The participant has positive feeling towards using the EHR	30
skeptical_attitude	The participant is skeptical about aspects if the EHR	17
access_rights	The participant talks about who may access the EHR	84
access_method	The participant describes methods to access the EHR	23
risks	The participant perceives something as critical	31

C Additional Results

Table 3: Table displaying the entities of participants mental models, their access right, and the storage location of the EHRs. 👁 denotes read access, ✏ denotes write access, and 🎚 denotes access management.

ID	Entities	Access to EHR	Storage Location
P1	patient 👤, doctors 🏥, server 🗄, health insurance 🏠	doctors 🏥, health insurance 🏠	server 🗄
P2	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	patient 👤 👁 ✏, doctors 🏥 if granted, health insurance 🏠 if granted	server 🗄
P3	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, national authority 🏛	doctors 🏥 if granted	server of health insurance 🏠
P4	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱, emergency doctors 🏥	doctors 🏥 👁 ✏, emergency doctors 🏥 👁 ✏	server 🗄
P5	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	doctors 🏥 if granted, health insurance 🏠	server 🗄
P6	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	doctors 🏥 if granted	server of health insurance 🏠, chipcard, smartphone 📱
P7	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	doctors 🏥 if granted, family, emergency doctor 🏥, family	server 🗄
P8	patient 👤, doctors 🏥, server 🗄, health insurance 🏠	patient 👤, doctors 🏥 if granted	server of health insurance 🏠
P9	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱, hospital	doctors 🏥 if granted, hospital if granted, health insurance 🏠	server 🗄
P10	patient 👤, doctors 🏥, server 🗄, health insurance 🏠	doctors 🏥 if granted	server 🗄
P11	patient 👤, doctors (in charge) 🏥, server 🗄, health insurance 🏠, smartphone 📱, pharmacist	patient 👤, doctors in charge 🏥 👁 ✏, pharmacist	server of health insurance 🏠
P12	patient 👤, doctors 🏥, server 🗄, health insurance 🏠	doctors 🏥 if granted, health insurance 🏠	doctors 🏥
P13	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	patient 👤, doctors 🏥, health insurance 🏠	server 🗄, App
P14	patient 👤, doctors 🏥, server 🗄, health insurance 🏠	doctors 🏥 if granted	doctors 🏥
P15	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	patient 👤 👁 ✏, doctors 🏥 👁 ✏, health insurance 🏠 👁 ✏	server 🗄
P16	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱, national authority 🏛	patient 👤 👁 ✏, doctors 🏥 if granted, health insurance 🏠	server of health insurance 🏠
P17	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	doctors 🏥 if granted	server 🗄
P18	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	doctors 🏥 👁 ✏, health insurance 🏠 👁 ✏	server 🗄, chipcard
P19	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, independent national authority 🏛	patient 👤 👁 ✏, doctors 🏥 👁 ✏	server of independent national authority 🏛
P20	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱, hospitals	doctors 🏥, hospitals	server 🗄
P21	patient 👤, doctors 🏥, server 🗄, health insurance 🏠, smartphone 📱	patient 👤, doctors 🏥 if granted	server 🗄