Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness

MELANIE DUCKERT, The IT University of Copenhagen, Denmark
LOUISE BARKHUUS, The IT University of Copenhagen, Denmark

Digital health data is important to keep secure, and patients' perception around the privacy of it is essential to the development of digital health records. In this paper we present people's perceptions of the communication of data protection, in relation to their personal health data and the access to it; we focused particularly on people with chronic or long-term illness. Based on their use of personally accessible health records, we inquired into their explicit perception of security and sense of data privacy in relation to their health data. Our goal was to provide insights and guidelines to designers and developers on the communication of data protection in health records in an accessible way for the users. We analyzed their approach to and experience with their own health care records and describe the details of their challenges. A conceptual framework called 'Privacy Awareness' was developed from the findings and reflects the perspectives of the users. The conceptual framework forms the basis of a proposal for design guidelines for Digital Health Record systems, which aim to address, facilitate and improve the users' awareness of the protection of their online health data.

CCS Concepts: • **Security and privacy → Privacy protections**; *Usability in security and privacy*.

Additional Key Words and Phrases: health; privacy; clinical records; e-health

ACM Reference Format:
Melanie Duckert and Louise Barkhuus. 2022. Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness. *Proc. ACM Hum.-Comput. Interact.* 6, GROUP, Article 11 (January 2022), 22 pages. https://doi.org/10.1145/3492830

1 INTRODUCTION

Following the past couple of decades' development of digital technologies, as well as the emergence of new ones, vast amounts of personal data are now being exchanged through elaborate systems and infrastructures, both in private and public sectors. This is especially true in the healthcare sector, where the development has resulted in an increasing number of different digital health technologies, making e-Health a well-established part of modern healthcare, at national and international levels [66]. E-Health systems refer to "health services and information delivered or enhanced through the Internet and related technologies" and are considered to be innovative trends in healthcare across the world, as the digitization of health data has improved the quality of healthcare [18]. The term therefore covers various types of health related systems from hospital management, through patient healthcare records, to digital pharmacy communication and independent providers' patient data. However, in this study we focus on digital health record systems that

Authors' addresses: Melanie Duckert, The IT University of Copenhagen, Copenhagen, Denmark, mela@itu.dk; Louise Barkhuus, The IT University of Copenhagen, Copenhagen, Denmark, barkhuus@itu.dk.

2573-0142/2022/1-ART11 $15.00
https://doi.org/10.1145/3492830

contain a detailed overview of a patients' healthcare, and can be accessed by authorized healthcare providers and the patient themselves. These systems are important to patients and healthcare professionals as they provide both health benefits, such as faster and more effective treatment, and reduce health care costs [5, 27]. However, while providing many health benefits, concerns about personal data protection, including information privacy, arise because of the risk of unauthorized access to personal health data, through the collection and transmission of such data within these systems. Such concerns can affect patients' willingness to disclose and share their health data, with potential critical consequences. For example, the U.S. Department of Health and Human Services (HHS) estimated that approximately two million Americans suffering from mental illness did not seek treatment as a result of information privacy concerns [31]. Information privacy, and in particular people's desire for control over their own data, is important in e-Health, due to the sensitive nature of health data. The awareness that health data can be compromised, directly affects people's approach to utilize and accept e-Health systems. If stolen or otherwise compromised, these data may have critical implications for patients [16].

The increasing number and variety of e-Health technologies and systems have also generated technological measures and legal agreements to protect users' personal data. In the healthcare sector, privacy-enhancing technology (PET) has been developed in an attempt to solve problems related to users' information privacy. This is done by applying a set of privacy principles to the processing of personal data, which helps to limit data collection and data specification. Another approach to protect personal information privacy is 'Privacy by Design'. This approach can generally be described as a way of integrating privacy features into the actual design specifications of a technological system, so that the fair information practices (FIPS) and the related guidelines are integrated into a product [10]. This approach aims to protect user information privacy while maintaining the efficiency and capabilities of the given technology.

The approaches to information privacy in e-Health systems are even more important today, where data protection of users' personal sensitive information, including health data, has become a legal requirement under the EU General Data Protection Regulation (GDPR). GDPR requires companies and public institutions to comply with specific requirements, in terms of handling and storage of users' data, as well as requirements for disseminating this to users of their websites or services. Failure to do so will result in financial penalties. Therefore, companies and institutions must inform their users about how their personal information will be used.

Several studies have contributed to the understanding of how to protect patients' digital health data [3, 39, 41], as well as understand their patients' concerns [1, 48], and studies have provided potential suggestions for various technical and legal measures [30, 63]. However, fewer studies address patients' approaches and practices in regards to protecting their own health data privacy, as well as staying informed of how and with whom their health data is shared. These practices have significant importance for the design of data presentation, design of personal health records, and more broadly design of e-Health systems. This study addresses digital health record systems from the patient's perspective, looking at aspects that are essential for informing users of how their health data is handled and protected. Based on an interview study with 16 patients with chronic illness or long-term illness we describe first their in-depth experiences with the national online healthcare personal record system and secondly their perception and concerns with the system and healthcare data more broadly; we then present our framework for understanding patients' perception of health data privacy, which can work as a basis for design of e-Health technologies. Our contribution of the framework aims to facilitate a better understanding of how to design e-health technologies.

2 RELATED LITERATURE

2.1 Digital Health Systems

Electronic health records (EHR) are generally used to describe personal health information that is captured and stored in digital records by both public and private organizations. Personal health records (PHR) contain the same information but are designed to be manged by the patients [28]. These, and related terms such as electronic medical records (EMR) and patient portals, overlap in their purpose and utility, why the terms are often used interchangeably [45]. But in our findings and results, we refer to the specific system in our study as a Digital Health Record system (DHR). The specific system will be described further down.

Different electronic health record systems have been developed around the world and in individual countries different services are exploited, e.g. medical records and personal health data (such as allergies, laboratory test results) [24]. A broad survey of EHR systems in 13 countries looked at success factors, and found that the most significant success factor was the commitment and involvement of all stakeholders of the system, including both medical, nursing and administration [21].

Information systems are introduced in many public organizations yet Anderson and Agarwal argue the healthcare context to be unique in at least two respects: risks inherent in the compromise of sensitive health information and the emotion linked to a person's medical state [1]. They examined the users' willingness to provide access to their personal health information (PHI) and how this is affected by different circumstances. Besides cognitive factors (electronic health info, privacy concerns, trust in the system) and risk scenario variables, (type of information, intended purpose, requesting stakeholder), they argued emotion as a conceptual factor affecting people's willingness to share PHI. For example, they found people with negative emotions involving their current health status to be more willing to disclose PHI and that the type of information does not have a significant main effect on willingness to provide access to PHI [1]. However, Lim et al found patients to be cautious about what information to share, due to assumptions about what actions the doctors might take, and that patients with multiple chronic conditions sometimes avoided sharing all information about their health despite its potential to be relevant to their healthcare [35].

2.1.1 Personal Health Information as Confidential Information. Personal health information (PHI) is by definition private information that most patients not only expect but also prefer to be kept private, except from appropriate users such as medical personal. As more data are stored in digital records, the security and privacy of the patients become paramount [19]. This confidentiality is also approached differently in different countries [3], for example, patients can request an accounting of the disclosure of their health information [19] or doctors cannot be allowed to access the personal health information without consent from the patient [3]. In the United States, HIPAA (Health Insurance Portability and Accountability Act) stipulates that patients can request an accounting of the disclosure of their protected health information by hospitals and other "covered entities" [19]. The UK limits the circumstances in which the law allows the use of patients' information without asking first, while the Netherlands requires consent from the patient for doctors to access information, similar to Portugal that also needs a clearly defined time frame [3].

2.1.2 Designing Electronic Health Record Systems. Several studies have addressed the design of EHR systems, both during the design process and after implementation. A recent study of large-scale implementations of a system in Norway illustrated the complex activities and participatory design methods in play, for the design and appropriation of the new EHR system [65]. Other previous research has contributed with implications for design of EHR systems that could enhance privacy [30]. For example, in some EHR systems, patients can individually choose which doctors can

access what content. Caine and Hanania proved "patients would like to have granular control over the privacy and sharing of information about them in their EMR" [8]. However, patient-controlled access can potentially lead to challenges as an ordinary citizen should be considered a non-security expert and are therefore not necessarily aware of the consequences of the actions. For example, by not being able to give permission to access some information, a patient can prevent the system from being effective and useful [61].

2.1.3 Health Systems as Collaborative Systems. Over the last few decades, the relationship between doctors and patients has been affected by the digitization of health care records. Previously only the physician directed the patients' care and decision-making about treatment [14]. However, the digitization of healthcare systems provided availability of information to the patients and contributed to the two-way communication between doctors and patients [37]. Enabling patients access to health information and their personal health records created a group of "informed, engaged, and empowered" patients, who are equipped to take part in the decision making [37]. EHR systems are therefore not only a work tool for the physicians but also patients [9], who additionally can be more actively involved in their treatment by for example effectively self-manage chronic illnesses [36, 37].

Collaborative health systems also brought several challenges with them and were met with skepticism from the health professionals [9]. The deployment required implementation of new ways of working [26] which could cause issues as the healthcare sector is a complex setting [40] and it could risk introducing new information problems for the healthcare professionals [42]. For example, information in EHRs often require the provision of professional medical expertise [12], which does not always meet the need for appropriately communicated health information to patients [14]. Patients might misinterpret the medical notes or test results, which for some people can create anxiety if they misunderstand the information [9, 17].

While the wider availability of more general healthcare information through the open Internet has also affected doctor-patient relationships [12], for example by patients more often attempting self-diagnosis, this part of the healthcare infrastructure was not part of our study.

2.2 Privacy Research

While a significant amount of research has addressed health care record keeping from a privacy perspective, the overall notion of privacy and trust is important to consider in order to understand the patients in a broader context. We therefore take a brief step back and review some of the relevant research into privacy issues among users of personal information systems more generally.

An article by Smith et al. presented an overview study of privacy research in information systems [52], where privacy was found to be approached majorly from a normative perspective and less from empirical descriptive perspectives. The paper highlights that privacy is often described as privacy concern, which is the entity of study in much of the related research. In this paper, we also focus on privacy concern as a central construct. However, while earlier studies of coarse grained data sharing preferences illustrated personal privacy concerns, more recent research includes a broader context. One framework that is very appropriate for understanding our results is Helen Nissenbaum's Contextual Integrity framework [43]. It takes its basis in how our everyday human life is governed by norms of information flow, those being cultural, ethical or moral norms. We are able to fluently transform our behavior according to these norms just as we appropriate our actions with people we have different relationships with. Contextual integrity describes a desirable state that people strive to obtain and maintain, by keeping (perceived) private information private according to the context. For example, people will readily share health information with doctors and providers, but are not comfortable sharing the same data with colleagues or employers. Several

studies have used Nissenbaum's framework for analysis, for example in an analysis of use of specifically tailored social media pages [51] or social media use of location sharing [4]. In this paper we also lean on Nissenbaum's framework for interpreting our results of privacy concern, specifically in a health care record context.

3 THE NATIONAL HEALTH DATA SYSTEM

Before describing our research method, we introduce the national healthcare record system utilized in Denmark where our study took place. In this section, we give an overview of Danish healthcare and the digital health system, which architecture has evolved over the last two decades.

The national health care system operates on three levels: the state, the regions, and the municipalities (national, regional, local levels). The national health data system is a centralized system for all medical systems across the three levels, from family doctors, through specialty doctors to hospitals. The National Health Portal, or 'sundhed.dk' as it is called, has existed since 2003 where it was rolled out as the centralized system combining information for both doctors and their patients. For example, citizens can find publicly available information on classification, treatments, waiting lists [55]. However, this first part did not contain personal records.

In 2014, the Digital Health Record was launched as a part of the online National Health Portal gathering all personal health information in one place. Before that, like most other pre-internet societies, the information was only available through doctors and hospitals, or through personal data requests. The Digital Health Record system contains online services for the citizens, who can access their personal health information, book appointments with their physician, and access medical data and prescriptions [55]. The access is divided into two: citizens and doctors from the national health sector. With the patient's consent, doctors can register, access, and share all health information across the three levels of the healthcare system, making the work with a patient more effective [32]. Besides medical professionals, also researchers and institutions can get access to biobanks and lab- or imagining systems [23]. In theory, all health personnel have access to all the patient's data, however, the system contains a strict control of who can access specific information and only a healthcare provider *assigned* to a patient, and where the patient has provided consent, can access it without being reprimanded or even laid off for inappropriate access. Only in cases of emergency, doctors are extraordinarily allowed to access a patient's health record without their consent, this is for example in cases of accidents or if the person is not conscious and brought to the emergency room [29]. For the citizen, the Digital Health Record contains all health data such as complete patient history, lab results, narrative journal keeping by doctors, and general prescriptions. Moreover, the citizen can register as an organ donor, schedule appointments with physicians, request prescription refill, and share health-related thoughts and experiences with other patients [23, 32]. The citizen accesses the Digital Health Record with 'NemID', a 3-factor authentication that is the digital signature used to log on to Danish internet banks, government websites, digital posts, and other online self-services. When a person logs in for the first time, they must give consent for the digital journal to collect, process, and display their personal health information, for example, a citizen's personal health number which is necessary to use the services and view the health data. This initiative is partly a consequence of the introduction of the General Data Protection Regulation (GDPR), a privacy and security law drafted and passed by the European Union (EU) [57].

Denmark has a Patient Safety Authority that manages safety concerns in the healthcare sector, including cases with data breaches and illegal access to patients' Digital Health Records. The Digital Health Record system contains the feature 'My Log' where the citizen can keep track of *who* access *what* data in their health records, however, according to 'sundhed.dk's' statistics from 2015, only 14 percent of the citizens knew about this feature, making it the least known and used feature in the

Digital Health Record system [56]. If a patient suspects a healthcare provider illegally has accessed their health records, they can register a complaint to the Danish Patient Safety Authority. Moreover, the regions conduct random samples to check for potential cases where healthcare providers have accessed health records without authority. Such cases have been published in Danish news media, describing general concerns that healthcare providers are 'snooping around' in peoples' health records [60], individual cases where the healthcare provider got a warning or, in very few cases, been terminated [34, 50], as well as discussions of privacy and if *all* healthcare providers should be able to access *all* citizens' health records [47, 53]. In general, Danish society maintains a high level of trust in government and the associated public organizations [6, 58] and digital solutions [49]. However, there have been cases with data breaches within the health sector: in 2015, 5 million citizens' personal health numbers were mistakenly disclosed to a Chinese company [59], for five years local employees could by mistake access half a million citizens' personal health information [62], and more recently, pregnant citizens' health data were shared with a company in the US without the women's consent [33].

In this paper we solely address people's interaction and practices with the Digital Health Record, however, the participants refer to it colloquially as 'sundhed.dk', the broader portal. To clarify that they mean their own health journal, being the part where the patient logs into their own health data, we refer to that part as their Digital Health Record (from hereon abbreviated DHR).

4 METHOD

Our aim in this study was to investigate the practices and concerns of frequent users of the Digital Health Record in relation to their personal privacy. In particular we wanted to know how potential data privacy concerns affected their use practices, or how user practices affected their perception of their personal data confidentiality. While it is often taken for granted that people are willing to provide personal health data to national healthcare systems, it is also increasingly obvious to the same people that personal health data is not always confined to the systems (in essence the databases) that are originally intended to be utilized for this specific data. Our initial inter-related research questions were therefore:

(1) How do users perceive the communication of the protection of their personal health data, within their digital health record?
(2) What types of information do users consider essential in relation to the protection of their health data?
(3) How can personal health data protection be communicated appropriately in an EHR system?

The study took a qualitative approach to examine users' perception of data protection of their health data according to their digital health records. The method was inspired by Grounded Theory [54] with emphasis on inductive strategies for theory development. This can be useful when studying areas where not much research has earlier been done [13, 54]. The research was conducted in accordance with "The Danish Code of Conduct for Research Integrity", which is the standard set of guidelines used for research using human subjects in Denmark; guidelines are based on EU standard and as an interview based study, the research study did not have to go through an internal review board as is traditional at US based universities.

4.1 Participants

We wanted to investigate practices and concerns of DHR among people with significant experience using their own health records and as such aimed to recruit individuals with reasons for this, such as chronically ill individuals, or people requiring continuous treatment of some sort. The participants were recruited by snowball sampling, where initial participants refer researchers to potential next

Table 1. Participant information

Anonymized names	Gender	Age	Disease/illness
Ann	F	28	Minor son with an undisclosed illness
Brenna	F	39	Genetic predisposition to cancer
Catherine	F	23	Genetic predisposition to cancer
Daniel	M	49	Undisclosed
Esther	F	26	Undisclosed
Freya	F	25	Arthritis
Grace	F	28	Arthritis
Harry	M	24	Undisclosed
Isaac	M	35	Undisclosed
Jennifer	F	21	Postural orthostatic tachycardia syndrome (POTS)
Kristopher	M	29	Respiratory disease
Lucas	M	30	Undisclosed
Martha	F	27	Skin disease
Nick	M	27	Mental illness
Oda	F	47	Cancer
Paula	F	27	Undisclosed

participants [2]. The recruitment was seeded through contact with a colleague of the authors who located further relevant individuals; these individuals further referred us to others, however, not necessarily with similar chronic illnesses. Two participants were acquaintances (but not friends) of the two interviewers. The recruitment criteria were based on significant experience with their own Digital Health Record (possibly in addition to their children's) and that they had significant reason to access the record, regularly. All participants suffered from a chronic illness and/or long-term illnesses requiring continuous treatments, e.g. asthma, POTS, cancer, which ensured they were in contact with the healthcare sector and had regular use of their health records. Due to the focus of the study, no prerequisites for the type of disease were set and no further questions into course and progress of illness were asked; for reasons of privacy, the specific illness and medical status will not be listed in the paper either. A total of ten women and six men, aged between 21-49, volunteered to participate in the study. While we did not have a particular age-limit in mind, we limited older age participants, due to increasing complexity of illnesses, and potential unfamiliarity with digital services. All participants were regular users of the system and had visited their DHR at least within the last six months. The participants have been provided with pseudonyms to maintain their privacy.

4.2 Interviews

We conducted 16 semi-structured interviews to gain an understanding of how users perceive the dissemination of the protection of their health data, according to their DHR, and what information aspects they consider essential in relation to the protection of their health data. Interviews lasted about half an hour and focused on users' perceptions of data protection, their experiences prior to accessing the health record, as well as their thoughts and perception of the responsibilities of others in relation to this.

To inform what information doctors can access, we interviewed the chief physician of the Department of Intensive Care at the national hospital. Together with a review of the health portal, this provided initial knowledge of the DHR system prior to the participant interviews.

To not predetermine the views of the participants, the interviews initialized with broad open-ended questions and minimal topic control. This allowed us to understand and capture the views of the participants and develop the 'rich' description desired for this study. To ensure a comparative process, the interviews were analyzed in parallel with the ongoing interview process which made it possible to continuously increase the focus of the discussion on the designated areas. To document the data, we took fieldwork notes and memos during the interviews which in addition all were recorded and transcribed. The participant statements included in this paper are based on their personal experiences and not second-hand experiences. All interviews were conducted in Danish and after conducting the analysis, the included quotes have been translated for this paper.

4.3 Data Analysis

Coding is a key element of Grounded Theory [54] and has been the data analysis method for this study. It is a systematic process starting in the early stages of data gathering, where each phase of the analysis builds up to the next and plays a significant role in the development of Grounded Theory. In this relation, we systematically followed Strauss and Corbin's [54] three coding levels: open, axial and selective.

The data gathering and analysis progressed in parallel; after each interview, two researchers collected indicators in the form of words, sentences, and statements from the data memos, observations, and interview transcripts. In the open coding we started looking broadly for themes related to the participants' perception of the DHR system. This was done in close collaboration and (the very few) disagreements were solved as the analysis went on. After that, the indicators were related and grouped into ten interconnected concepts. Two researchers reviewed these concepts through axial coding, which specified three main categories composed by the ten concepts as subcategories. During this process, we moved to selective coding as the overarching theme of *privacy awareness* was identified. The categories were organized into a figure from which a conceptual framework was developed.

We first present our results structured through the categories we extrapolated out from the data, before presenting the framework. The ten concepts were: *the fine print; increased data protection; a no-choice system; responsibility; fear of data leaks; transparency; who, what, why, and how; (lack of) knowledge and understanding; unknown risks and consequences; emergencies.*

5 RESULTS

In this section we present the overall findings from the interviews. Our findings are separated in three parts, based on the categories developed in our analysis. They provide the base for our framework that is presented further down.

5.1 Context of Information Sharing

One of the main subjects discussed in the interviews was the context of the health information sharing, in the most simplistic sense, who, what, why, and how: the perception of who had access to what data and how they accessed that data about the participants. All participants expressed, in some way or another, that they had no clear idea of *who* in the healthcare sector had access to *which* part of the their health records. Both participants who were very concerned about sharing their health data in general, and participants who expressed less concern, were unclear about which types of health data the different healthcare workers could access. Two participants, Jennifer and Isaac, reasoned during the interview that, at least in theory, all healthcare personal could access their

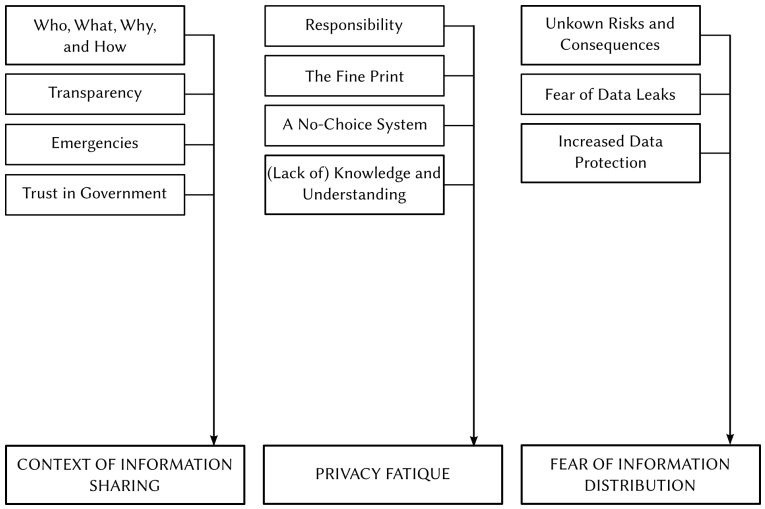

Fig. 1. Categorization Scheme

health data. Their guess was based on their contact and experience with the public health services and not based on digital information in the DHR. This reflects a potential lack of information and transparency in relation to personal health data at the DHR, a missing transparency that was also commented by Ann, Freya, and Kristopher. Moreover, participants were uncertain that their own consent provisions were correct. Kristopher for example described this doubt about who can actually access his health data: "[I]t feels like most [health personnel] can access [the data]. Also, even if I have to give consent and tick off who can access this information, I can quickly tick the wrong box and click another person who I was actually not interested in being able to have this information, who then suddenly has access to it. You somehow lose control over who knows what about you. I don't feel good about that actually."

5.1.1 Contextual Access. While the participants did not have a clear understanding of what information health personnel can find through the Digital Health Record, they also expressed doubt about the granularity of that information, such as the actual content of data entries as opposed to just visit data to, for example, a psychiatrist (e.g. Kristopher). They commented on three types of sensitive information: sexually transmitted diseases (STDs), mental health/illness, and physical/sexual abuse. Freya for example expressed some concerns: "for example mental health diagnoses, there is stigma in relation to those. Also, if there was a random doctor who could scroll through five different STDs [in the DHR], or whatever, that would not be that cool." The participants seemed to be more concerned about judgement from a doctor, than accepting how a full picture of a person's health history would be potentially useful for the doctor.

Since a doctor can access a patient's full medical history, three of the participants were afraid to be seen as hypochondriacs (Grace, Jennifer, Nick) and said they would be reluctant to share all relevant information with a physician (Jennifer, Nick). Jennifer for example, feared being stigmatized or not taken seriously by a physician if this doctor, based on her medical history, made presumptions of her current medical status. Jennifer elaborated that she did not even want another physician, who were also connected to her regular medical center, to know about all her health data, "I went to the physician with something that had to do with my illness, but not with sleep problems which are also a part of POTS. And he said to me 'I can see that you get sleeping medication' – out of

the blue! Then he said to me 'why do you get that?', well, because I can't sleep I say to him, 'but you're very young that can't be right' [the physician answers], and then he writes 10 tips on how to sleep well from the Danish Health Authority. And I just felt, that was crossing my private sphere, that [the physician] could look in my [DHR] and see my prescriptions." Despite that the physician legally accessed Jennifer's DHR, she felt her privacy violated because the doctor could see health data that was unrelated to the main reason she was there. This allowed the doctor to question previous decisions made by other doctors and putting her in a vulnerable position where she had to defend medical choices made by other doctors.

Some of the participants suggested that the access should be contextual (which it to a certain extent is already today, but this was not clear to them): "I think it depends on the situation, [who should have access] and it is difficult to define, because several different situations can occur [...]. There should have to be a reason for [the health personnel] to access [the DHR], and if they kinda have been informed that I somehow have given my consent for them to go check my record, if it can help them or do something for the hospital. But I don't think they should do it without reason" (Ann). Four participants preferred to manually give their consent for new doctors to access a patient's DHR, however, they also recognized that this could result in new challenges, for example in case of emergency, where most of the participants wanted all health personnel to have access. Nick described the shared access across all levels of the health system to provide 'a feeling of safety'.

5.1.2 Trust in the Government and National Health Care Sector. Overall, the health data environment was perceived by the participants to provide a lack of control over sensitive personal data, yet, they were 'forced' to follow the principles of the DHR that were provided to them, despite a non-transparent system of stakeholders, participants and confusing consent provision. While they expressed these critiques, 11 of the 16 participants still said they had trust in the government and the national health care sector. They argued that "when it's handled by the government, I have reasonable trust that they treat my data properly" (Isaac), "when I access with NEM-ID (the national digital signature), then I have a general assumption that it's a [platform] with good security. [...D]octors have a duty of confidentiality, as long they [access my DHR] as [authorized health personnel] they have a duty of confidentiality" (Grace), and "I expect competent personnel. If you're a nurse then you also have an idea of what this entails, so yes, I'll say that everyone [with authorized access] can access my data" (Harry). The participants, therefore, showed trust in the data sharing principles on the DHR and the health personnel who accessed it, despite them not being aware of who this was. Paula described: "I'm not aware of who has access at all. But it's because I trust the [security] and control. I believe that the people who need access have access". The contrast between how the participants described a general trust in the system and that they still claimed to have privacy concerns, yet not exhibiting privacy protecting behavior, was found to be closely related to privacy fatigue, an issue elaborated in the following section.

5.2 Privacy Fatigue

When asked about privacy issues in regards to the Digital Health Record service, all participants referred to the privacy policy and the declaration of consent on the service. We found a consensus among the participants that managing these policies and consent was "time consuming", "insurmountable" but also "unimportant". For example, Lucas said: "You are just so used to seeing it, so you just don't care, you just want to move on to the [health records]. I wish I was better at thinking about it, but I'm not. It has just become such a standard.". Similarly, Freya reported: "Yes, if you had the time and felt like it, then there is a lot to read - but you rarely feel like that. And I also think that, from my perspective, it has not been communicated, it had just been put out in a way so that no one bothers to read it. [...I]t could be better communicated, in an easy-to-understand

way." Other participants expressed confusion and insecurity of what the new GDPR law meant for their own health data. Catherine expressed: "I'm really confused when it comes to the new data legislation, but off the top of my head I would agree [that such data legislation is good], I always think it's good when the regulations are being tightened, especially because the overall technological development has led to a lot of the legislation. But I must admit that when I look at that GDPR, I get confused about some of the regulations."

The participants seemed to navigate the consent and privacy policies through mentally filtering out, due to what is often referred to as security- or privacy fatigue [22]. Where security fatigue is a notion that describes a person not adhering to required or preferred security measures, privacy fatigue is the inability or lack of effort in making decisions regarding online privacy. Privacy fatigue means people want to minimize effort in decision making [11]. Our participants suffered to a certain extent from privacy fatigue in their management of privacy settings such as whom were able to access what data in their DHR, or even by not trying to find out who had access to what data in order to consider if they thought that was right. One very clear articulation of such privacy fatigue came from Ann: "Right now, I think that organizations' [...] answer to GDPR is clearly these privacy policies and consent statements; to me, it becomes just another habit for us when we access something digitally. That we just press 'yes', but we don't read the things, we obviously don't read what it says, we don't even read what we consent to" (Ann). She related the management of healthcare data on the official system with broader private systems, for example websites where she just ticked yes to all services, and perceived that this was the norm for other people as well. As such, the GDPR imposed consent tick-box influenced the attitude towards more personal health data management.

5.2.1 A No-Choice System. The finding that the participants felt that they had no energy for maintaining or being constantly aware of their health data sharing, closely related to how the system was a "no-choice system", a mandatory healthcare record system, for managing personal (or children's) health data. Kristopher said: "I feel like it's kind of a service one is forced to use, something you somehow is forced to consider. Exactly because [the service] is not going to go away. It is a bit like the e-box or digital post [a standard government communication tool], it does not disappear. This is the way things are here and now. You are forced to learn to live with it. And forced to feel safe about it because else... [...] Sure, there is a possibility that it will get hacked, but there is also a possibility that it won't. And if you have to [constantly] worry about your personal information and your personal data gets [stolen], then you wouldn't get to spend time doing anything else" (Kristopher). Others were not as sceptical but reasoned that "they had nothing to hide", or did not have any "embarrasing" health information that they feared would get into the hands of the wrong people. Daniel for example explained that although the healthcare record system was a more or less no-choice system, he had nothing to hide and that he trusted that the healthcare data was being kept and stored confidentially.

5.3 Fear of Information Distribution

One reoccurring issue that related to participants' privacy concerns was the fear of personal healthcare data being distributed or accessed by irrelevant people. Interestingly, most participants started the interview by expressing that they had rarely been concerned, but as the interview progressed, likely as a side effect of talking about healthcare data privacy (this is also discussed in our section on limitations), participants expressed different concerns. The concerns were of two types, concerns about illegal access, for example through hacking or access by inappropriate or undesired *other* health personnel. We discuss each type in turn.

5.3.1 Illegal Access to Data. The subject of hacking was a recurring theme by around half of the participants, for example Kristopher expressed: "When you hear about all that's going on in the public debate and news and such, then I become more and more sceptical about sharing this personal information. Because you hear about how the [social health numbers] suddenly have ended up in the Chinese Embassy [1]. Or that somebody suddenly has access to one's [social health number]. Well, or that there has been some error in a system and they [the social health numbers] got into the wrong hands, if you can say so. In that sense I'm not super happy about the personal information sharing during this time, with 'the more [data] being available the better'. I can see it is clever, but the negative things weigh actually more than the positive things about it." Later the same participant went further and mentioned how he sometimes considered *not* telling his doctor something, due to the unknown consequences of this data being written down, and then later being available through illegal access: "But I will also admit that there has been a couple of times where I think, that I have to hold back [in terms of providing information] to my doctor. Because if [...], in a future scenario, one could imagining that others get access to these data, somehow. It could be a future employer or Russian hackers who sell the information [...]." (Kristopher)

Esther also expressed such fear but did not distinguish as clearly between illegal hacking and data sharing across (public) systems: "I could feel a bit pressured to hold back from fear that someone, who can access my [health] record and thereby make a decision that I don't have an option for something, for example adopting [a child]. I mean, if someone has some illness that means they cannot adopt, that's something to fear, that an adoption agency or who it is, should get access to my digital health record and see that because I once had some illness, then I'm out. That, I don't like. That might mean that I wouldn't tell everything about my health to my doctor, from fear that something would be written forever in some [health] record, that someone from the outside, who perhaps already now has access to, or perhaps in the future gets access to." Overall, most participants did not dwell on illegal access to health data, such as through hacking, but emphasized concern of a more legal but inappropriate nature.

5.3.2 Legal Sharing Concerns. A fear of legal sharing of personal health data was also presented, exemplified here by Esther: "I am a bit worried to find out that all authorized doctors or nurses suddenly have access to [the health record]. On the one hand, I would like to know it, on the other hand, I'm a bit scared of the answer [of who can access her health record]."

The DHR log shows who has accessed the patient's record. But since it is not communicated clearly before login to the DHR system who can see personal information, the log did not seem to create trust or certainty among the users. Brenna for example explained that she had "an insidious suspicion that there are ways to access [her personal health data] which is not visible to [her]". Due to the concern of how encompassing the data sharing actually is, some of the participants claimed to retain information from the health personnel (e.g. Jennifer).

Four of the participants, Esther, Grace, Kristopher, and Martha, commented that they might hold back health information due to fear of who will get access to this information in the Digital Heath Journal. Grace commented on the the duality of the benefits and worried: "It would be terrible if you feel the necessity to hold back, exactly because you don't trust that what you say will be kept confidential. Your information is important for your health, really actually for you life". Relatedly, Martha said "the more information, the better the doctor can do to help you. If you keep something back about your health, then there is a chance to be misdiagnozed".

[1]The participant referred to the case where the Chinese Visa Application Center mistakenly received two CDs, which contained unencrypted information about 5 million citizens' health data and personal health number [59].

5.3.3 Weighing the Bad Against the Good of Digital Information. During the interviews, five of the participants commented on the positive and negative consequences of moving from paper based to digital health records. Jennifer said, "And I think, personally that if I should have my health records on paper, then it would be an encyclopedia; I mean, just a really thick pile. I wouldn't be able to manage that myself. I think it is better that it is digital. I also think that a hacking attack, if it hit me and my [personal health number] then I don't know what they would use it for. But it is of course a risk [...]. But I think in relation to saving lives, not mess up too much in some random archive in the wrong place [...] then I think you can keep track of it better digitally". Isaac commented on the advantages of storing information digitally, "I don't really know if it was more safe with the paper records, because there were many things that were lost. And that is the good thing about it being digital, that it does not get lost in the same way as it did back then. But there is of course and increased risk [of information leak], maybe you should make an extra effect on [improving security] because it is more accessible now [compared to paper records]." Thus, the participants felt secure in having their health information stored digitally compared to the paper records, yet, experiencing new concerns about whether they could rely on the privacy and security measures.

The participants commented on several privacy concerns; however, they still presented trust in the government, the healthcare personnel, and that their data was securely stored. Although this did not made them investigate the privacy measures in the DHR system and several of them were not aware that they do have the option to personalize the settings for information distribution. For example, Ann showed strong opinions about privacy and the protection of health data and said that she would prefer to manually provide new health personnel consent to access her DHR. However, she also admitted to never have considered looking into the privacy and access settings related to this and available in the DHR. We found that participants viewed health data as significantly private information; they described it as "a part of my private sphere" (Ann) and that they contain "some of the most intimate information about us" (Harry). Most of the participants trusted the government to keep this data safe and that the authorities made sure that only authorized and relevant personnel accessed it. Yet, several of them feared potential illegal information distribution or access to the DHR, just as a few of the participants commented on discomfort in relation to doctors who legally accessed (what they perceived as) non-relevant content in the DHR. The results indicate that this was grounded in missing transparency and communication of information distribution and privacy within the DHR as well as from health professionals.

5.4 Limitations

The study as we conducted it has some limitations and before presenting the framework, we comment on some of the most important ones. First, our recruitment strategy was based on snowball sampling. While this method is advantageously and often used for recruitment within a community [2] or hard-to-reach people [20], we chose this approach to locate people with chronic and/or long-term illnesses but without limiting the study to one specific type of disease. A person's medical state can be a sensitive subject, thus we, despite this not being the focus of the interview, prioritized to locate participants from this chain-referral method. This approach can result in a sample with questionable representativeness [2], however with a majorly qualitative approach, we consider the findings of the study valid for exploring users' perception of privacy when using their DHR.

The interview study investigated how the participants perceived the protection of their health data and what information aspects they considered relevant. The interviews therefore included questions about their perceived privacy, which some of the participants had not thought about prior to the interview. Consequently, some participants' initial answers represent trust in the system and the healthcare personnel, however, we cannot disregard that during the interviews

the participants expressed more worries about potential privacy issues, at least partly due to the prompting. Moreover, the participants might be influenced by the news media coverage of prior cases with healthcare personnel who have accessed patients' DHRs without authority. These incidents are rarely proved, and several of the claims presented in the Danish news media, therefore, built on suspicions of unauthorized access and not proven illegal activities (however, this does not mean that the suspected activities are authorized only that it is not proved to be illegal). Nonetheless there have been cases with data breaches where personal health data have been disclosed to external entities by mistake or without consent [33, 59, 62]. In general, there is a high level of trust in the Danish governmental services, which was also confirmed by the participants though they argued for privacy concerns with the design of the DHR system.

6 DISCUSSION AND FRAMEWORK

The findings lead to our conceptual framework on understanding privacy issues in relation to DHR access from patients' perspectives. Our interviews revealed that patients were keen to keep their personal health data protected, but also that they expected a responsibility from both themselves as users, the health personnel as users and from the supplier of the DHR system. The framework derived from the main and subcategories presented in findings. We now present the three categories that together form the framework; the framework itself is illustrated in figure 2. Each part leads to coarse grained design guidelines explained in the end.

6.1 The Fine Print

The first part of the framework describes people's interaction around consent for sharing data within the DHR system, both in terms of giving consent, understanding what they consent to and worrying about what they have consented to in terms of personal health data sharing. Not unlike previous literature focusing on peoples' actual engagement with Terms of Service (TOS) documents and notifications [7, 25, 44], we found that the consent form in the digital health record was generally "time consuming" and "unmanageable". Privacy policies were considered to be for the sake of the health professionals, for which reason it was expected to be appropriate and functional; however, the patients were not motivated to read them. The primary reason for this was that the policies tended to be long, text-heavy, complex, and bound by strong legal language that the users are not able to understand. Other reasons for not reading them included vague language and expressions, format and font, or users' prior trust (or lack thereof) in the public health sector. Similar to other websites, acceptance of the TOS is usually a prerequisite for accessing a website or service, which was why most users accept the agreement almost automatically and these terms are rarely considered reasons to avoid a site.

Distribution of personal health information through DHR systems caused a certain level of concern and fear, but where most consent forms on the internet such as social media, entertainment or web shopping services had few predicted potential consequences, the DHR system gave users the sense that consent decisions had potential for life-and-death consequences. This perception made the consent statement even more unclear and confusing.

The foundation of the privacy policy and consent form on the DHR system is the EU Data Protection Regulation (GDPR), which requires organizations to be open about what data they gather and why. In return, consumers can request access to see which data organizations possess data, as well as have the ability to update and remove personal information if necessary. However, the Data Protection Regulation can be misunderstood by users if they do not know, or are unaware of, what it means for them, as illustrated by several of the users being confused by what was directed by the GDPR law, and what was directed internally from the DHR system.

Our findings indicated that when a website's privacy policy is presented to users by default, they might spend considerable time and effort reading it. On the other hand, when users have the ability to accept the terms and conditions of the site without reading a policy, they will generally refrain from reading the document. Even when users decide to click on a non-mandatory link to read the policy, they spend much less time and effort reading the document. One possible explanation for this lies in choosing to click on the link. It is possible that clicking on the link to read the policy served as a source of security for users. By clicking on the link, a feeling of having made an active effort to be informed is obtained, and after doing so, there is no longer a need to actually read the document. In the overall perspective, having people read the 'fine print' will always be a challenge, and our framework highlights the importance of designing for a clear understanding of what has been consented to in terms of data sharing.

6.2 Context

The second part of the framework relates to the broader context of access to personal health data. The question of when, and by whom, a patient's health information legally can be accessed was uncertain for all the participants. In particular, we found the question of *who* has access to a person's DHR to be a concern, especially since none of the participants were certain about this. Despite that, the DHR system allows the patient to select who to provide access, which was also recognized by several of the participants, they did not seem to feel confident that they had made the 'right' choice. This relates to the findings of Trojer et al. who found patient-controlled access to be a concept that put the citizen in a position to set privacy preferences but possibly without them being aware that their choices can prevent the system, and the healthcare personnel, to work effectively [61].

In order for the patients to feel more equated in management of their health data, the participants expressed a need for a more user-centered approach to the digital healthcare portal overall. They also wished that health authorities would explain their data collection and practice as a significant part of their online communication. What was essentially requested was that if personal health information was collected, the following was made clear: The names of affiliates, and external third parties with whom the information is shared, what data is shared with them and how to opt out of this. Some of the informants mentioned specific terms of consent requirements: information about the purpose of the policy, what information has been collected and how it will be used, as well as user rights regarding their health data, how the health service will protect their data and who to contact for further information on this. Additionally, a desire for control over one's health data was mentioned, including personal choices of who can see one's health data, as well as what data is shared with different health professionals. It was clearly important to participants that their health data is not shared with any third parties, such as pharmaceutical companies. As part of the people's desire for self-control over their health data, the participants commented on different aspects: gaining insight into what information is available about them, where there were varying reasons for this all built on fear, such as to see what other health professionals might have shared (Kristopher), to see what consequences these health data may have (Esther), and to make sure that what is stated in the health record is correct (Nick).

Generally, there was a wish to feel more secure about data protection in the participants' individual DHR. This was especially due to the fact that the health record was viewed as a private sphere where personal health information was stored for the individual patient and his/her doctor(s). However, people were aware that their health data could also be used for various purposes, an acknowledgment illustrating their concerns in relation to targeted data sharing. The participants would prefer the public health service to handle personal health data more transparently and responsibly in relation to how health data is stored, protected, and managed.

6.3 Risks and Consequences

The third part of the framework concerns the risk and potential consequences that people have to consider when using a DHR system like this. While the risk of hacking might not feel big, the participants all acknowledged their own lacking ability to assess data risk. Several of them would like to critically assess their digital health information, however, they did not feel sufficiently informed to be able to offset such risks and consequences. The majority of the participants had not familiarized themselves with the possible consequences of health personnel or other outsiders getting unauthorized access to their health data, yet, this was considered to be a lacking information aspect in relation to the protection of health data. Despite information on the digital health records' right to access and handle personally sensitive information being disseminated on the web portal, the participants did not have a deeper understanding of risks and consequences, and therefore did not feel competent to articulate a position on their own data security.

The balance between the perceived benefits and consequences of sharing digital health data was frequently brought up in the interviews. Quick access to one's own health information was important for the participants who compared it to the alternative of contacting health authorities directly, e.g. hospitals, for information regarding their health record, which was distinctly preferred to be done digitally. Holding this advantage up against the risk of potential intrusion (that being illegal measures or simply mistakes in consent) into personally sensitive information, it was clear that the benefits carried the greatest weight. As some of the participants expressed it, the associated risks is "worth it".

The participants accepted that digital storage of health information would make it difficult to keep most of the information private. Thus, it was referred to as one's own responsibility if the user did not have a sense of how data storage technically operates in the DHR system. Therefore, information about the technological aspects of health data sharing was definitely a missing aspect that should be communicated through the broader DHR portal.

6.4 Privacy Awareness

The notion of privacy awareness has been used before, for example, Pötzsch [46] and Malandrino et al. [38] defined privacy awareness as the users' understanding of how and what personal data is processed, used, and shared. This definition relates to our category 'Context' in the framework presented in this paper. Deuker on the other hand, described privacy awareness to include people's ability to identify risks associated with disclosure of their personal information [15], which relates to our category 'Risks and Consequences'. However, in our study we found additional privacy aspects that should be considered when designing DHR systems. We do therefore not limit the conceptual framework of privacy awareness to 'inform users' but also consider their needs and judgment. When making sure people are 'privacy aware' we could assume that the user will make decisions that reflect their own privacy attitudes, yet this is not always the case which is why several factors must be considered, such as gains related to data sharing [46]. So while others have described privacy awareness to cover several individual aspects, we conceptualized these factors in a framework in relation to DHR systems.

The relationship between the three categories of the conceptual framework focuses on establishing and maintaining *privacy awareness* to increase the understanding and assurance of users' data protection. Privacy Awareness in our case is the users' perception and recognition of the DHR system's communication about data protection. It is dependent on both the user (because they decide what parts of the system to access and read) and the content, as neither should be seen as a separate entity. Privacy Awareness is thereby a condition of the relationship between the DHR

portal, users and content material, in response to the person's own agreement for allowing and storing their health data in the DHR system.

Privacy Awareness in this way depends on the users' knowledge, or lack thereof, of who can access their health data and their active level of commitment. The three mutual information aspects of the dissemination are critical: (a) in what context, covering who can access the data, what data is accessed, and the purpose of any data sharing and how this takes place; (b) the user's ability to understand "the fine print" in the sense of the regulatory guidelines applicable to the web portal; and (c) the ability to assess the potential risks and consequences associated with sharing and the storage of health data on the web portal.

While our framework is developed for health data privacy, it relates to other privacy frameworks for data sharing as well. Wisniewski and Page categorize a number of privacy frameworks within HCI in five categories: Privacy as Information Disclosure, Privacy as Interpersonal Boundary Regulation, Privacy as Contextual Norms, Privacy as Affordances and Design, and User-Centered Privacy and Individual Differences [64]. Our framework falls within two of the categories, and connects these through our case of health data: Privacy as Information disclosure and Privacy as Contextual Norms. The first category of frameworks and theories relate to how privacy is viewed through a lens of concern for information disclosure, such as the fairly simple collection of personal information through web-services (for example social media or online shopping) that can potentially be misused or passed on to unknown parties. These type of theories also include the 'privacy paradox', which indicate that "users may not always weigh costs and benefits in what one might consider to be a rational way." [64] While our study did not find excessive representation of the privacy paradox, the part of our framework "The fine print", illustrated how the presentation of simply what is being shared (per default), what information is being disclosed, was useful for people's sense of privacy awareness. Similarly, the "risks and consequences" that made up another third of the framework belongs in the category of information disclosure. Being informed and aware of potential risk and consequences leads to a lower level of concern for withholding information due to privacy concerns. Even if risks are still there.

Finally, our notion of context relates to the category of frameworks of Privacy as Contextual Norms. The framework Wisniewski and Page mentions are rooted in norm-based theory, in particularly Nissenbaum's Contextual Integrity [43]. This framework prescribes how contextual factors and social norms are "critically important when idenfitying appropriate information flows" [64]. In our study patients expect to share health data with their doctors and healthcare workers, yet with the lack of transparency in a digital system, it is never completely clear who has or in the future will have access to the digital information. Health data is characterized by being acutely personal, yet in reality as we saw in the findings, some information is more sensitive than other. An allergy might not be characterized as sensitive, where past STDs are considered very sensitive information. If this information is taken out of context, the person's sense of contextual integrity is threatened. The coarse granularity of consent provision, illustrated an unpredictable future context for the patients and they will then rather withhold information. People's contextual norms were created and upheld by emotions, a cultural understanding of a national collective healthcare system, as well as a general trust in government; still the norms had not been explicated yet, other than through consent forms and terms of service information documents available. Contextual norms were already built into the system to some degree. While people were not very certain of who could access their DHR, and they often believed it was "everybody", it was in reality much more constrained. This type of framework showed to be useful in gaining a deeper understanding of how DHR users' concerns emerge and how upholding norms for personal data sharing (for example that secondary private providers do not necessarily have access to irrelevant health data) is important

for designing and implementing DHR systems. We now discuss how to design or adjust future DHR systems with this framework in mind.

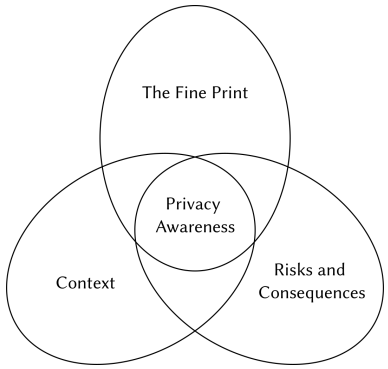

Fig. 2. Framework

6.5 Design

The conceptual framework lead to broad guidelines of how to design DHR systems that protect patients' personal health data. The three categories of the framework deal with different considerations in order to create awareness of information privacy, however, they will have some overlap. The categories are therefore supplementing each other in the shared goal of creating privacy awareness.

"The fine print" describes the users' experience and perception of the privacy policy on the overall DHR portal. In a design context, there are several aspects that can be included to support a more user-focused accessibility, as both visual and linguistic elements influence users' experience of the privacy policy. In addition, "the fine print" constitutes the users' path to information about data protection. The consent form contains essential information on what and who the DHR provides data access to, yet this is not the patient's primary source of information on data sharing. This information can be detailed and formally written, making it challenging for the common citizen to understand. A focus on, for example, visualization of this information can help the users' experience of what is important.

The category "Context" relates to the users' lack of knowledge of dissemination around the protection of their health information. Communication of this information is therefore a core area where the focus must be on the users' ability to relate this information to their personal information privacy. It is not only a question of whether the information is available on the DHR, but the focus should be on how the users experience this information. For example, if the option of personalized access control does not necessarily meet this need, then it is instead important to communicate the consequences of the choices. In this way, the broad topic of transparency can be considered. Transparency does not limit to the phrasing within a privacy policy but can also cover what measures are being taken to make users aware of how their data is used. For example, we found that an "active log", which notifies the users about the distribution of their data, made the participants feel informed about the sharing of their health data. The log is available on the DHR system, however, the user has to click through the website to find the information as no features indicate new activities (e.g. that someone has accessed the records).

The users' fear of potential risks and consequences is affected by the overall communication of data protection. It is formed by the users' experience of information privacy risks, the benefits of sharing data, and if this makes the user able to weigh the gains against the consequences of their

chosen privacy settings. Dissemination of data protection should make users aware of and able to assess any information privacy risks that may be associated with the use of DHR systems so that they can make informed decisions about their data. As technology evolves, the information about this must also be made available so that users can gain insight into potential changes around their information privacy conditions, changes that need to be made explicit in the design of the DHR system.

7 CONCLUSION

In this paper we set out to explore privacy concerns of frequent users of a national digital health record system, in terms of their personal health information. Through interviews with 16 participants with chronic or long-term illnesses, we described how they are very uncertain of who and what of their personal health information is shared in different contexts. While they were concerned by "wrong" people getting information, they had no other suggestions for managing this than to withhold information. Our findings lead to a conceptual framework that describes three aspects of Privacy Awareness, which in sum can assist in a better understanding of DHR system users' worries and reactions, as well as suggest how to appropriately design for these systems. In conclusion, the complexity of these systems and the sensitive nature of health information, lead to requirements for clear communication of data sharing context and consent descriptions and visualizations.

While the study was conducted in a context with high level of trust in government and a significantly lower set of stakeholders in health care infrastructure compared to countries that employ vast systems of insurance and private providers (e.g. the United States), we argue that our findings can still inform a broader spectrum of contexts. In one sense, Denmark is an idealistic setting for such study, because the health care system is simplistic compared to other countries, and it is therefore only appropriate to believe that other contexts would introduce more complexity to the framework presented. It is significantly more important to design for sensitivity in the systems when managing even more stakeholders and when users have more complex system infrastructures to navigate. Still, we hope to conduct future work within another context of health care infrastructure to complement the research and broaden out the framework.

ACKNOWLEDGMENTS

Thanks to Susanne Kristiansen og Sofie Rømer for assistance with the interviews and analysis. We also thank the participants who took the time to talk to us about their use of the health record system.

REFERENCES

[1] Catherine L. Anderson and Ritu Agarwal. 2011. The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Info. Sys. Research* 22, 3 (Sept. 2011), 469–490. https://doi.org/10.1287/isre.1100.0335

[2] Earl Babbie. 2004. *The practice of social research.* Thomson/Wadsworth.

[3] Gustavo Marísio Bacelar-Silva, Carlos Miguel Oliveira Vicente, Margarida David, and Luís Antunes. 2011. Comparing Security and Privacy Issues of EHR: Portugal, the Netherlands and the United Kingdom. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '11).* Association for Computing Machinery, New York, NY, USA, Article 57, 4 pages. https://doi.org/10.1145/2093698.2093755

[4] Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12).* Association for Computing Machinery, New York, NY, USA, 367–376. https://doi.org/10.1145/2207676.2207727

[5] RC Barrows and PD Clayton. 1996. Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association : JAMIA* 3, 2 (1996), 139—148. https://doi.org/10.1136/jamia.1996.96236282

[6] Robert J. Blendon, John M. Benson, and Joachim O. Hero. 2014. Public Trust in Physicians — U.S. Medicine in International Perspective. *New England Journal of Medicine* 371, 17 (2014), 1570–1572. https://doi.org/10.1056/NEJMp1407373 arXiv:https://doi.org/10.1056/NEJMp1407373 PMID: 25337746.

[7] Rainer Böhme and Stefan Köpsell. 2010. Trained to Accept? A Field Experiment on Consent Dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2403–2406. https://doi.org/10.1145/1753326.1753689

[8] Kelly Caine and Rima Hanania. 2012. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association* 20, 1 (11 2012), 7–15. https://doi.org/10.1136/amiajnl-2012-001023 arXiv:https://academic.oup.com/jamia/article-pdf/20/1/7/6087987/20-1-7.pdf

[9] Åsa Cajander and Christiane Grünloh. 2019. Electronic Health Records Are More Than a Work Tool: Conflicting Needs of Direct and Indirect Stakeholders. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300865

[10] Ann Cavoukian, Angus Fisher, Scott Killen, and David Hoffman. 2010. Remote home health care technologies: how to ensure privacy? Build it in: Privacy by Design. *Identity in the Information Society* 3 (08 2010), 363–378. https://doi.org/10.1007/s12394-010-0054-y

[11] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81 (2018), 42–51. https://doi.org/10.1016/j.chb.2017.12.001

[12] Andrea Civan, David W. McDonald, Kenton T. Unruh, and Wanda Pratt. 2009. Locating Patient Expertise in Everyday Life. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work (GROUP '09)*. Association for Computing Machinery, New York, NY, USA, 291–300. https://doi.org/10.1145/1531674.1531718

[13] John W. Creswell. 2018. *Research design: qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.

[14] Raisa B. Deber. 1994. Physicians in health care management: 7. The patient-physician partnership: changing roles and the desire for information. *CMAJ : Canadian Medical Association journal = journal de l'Association medicale canadienne* 151, 2 (July 1994), 171—176. https://europepmc.org/articles/PMC1336877

[15] André Deuker. 2010. Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services. In *Privacy and Identity Management for Life*, Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, and Ge Zhang (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 275–283.

[16] Molla S. Donaldson and Kathleen N. Lohr. 1994. *Health data in the information age: use, disclosure, and privacy*. National Academy Press.

[17] Gudbjörg Erlingsdottir, Cecilia Lindholm, and Ture Ålander. 2014. eHealth services, patient empowerment and professional accountability - An empirical study on the changing patient-doctor relationship in the digital world. In *International EIASM Public Sector Conference; Conference date: 02-09-2014*. 1–21.

[18] G. Eysenbach. 2001. What is e-health? *J Med Internet Res* 3, 2 (18 Jun 2001), e20. https://doi.org/10.2196/jmir.3.2.e20

[19] Daniel Fabbri, Kristen LeFevre, and David A. Hanauer. 2011. Explaining Accesses to Electronic Health Records. In *Proceedings of the 2011 Workshop on Data Mining for Medicine and Healthcare (DMMH '11)*. Association for Computing Machinery, New York, NY, USA, 10–17. https://doi.org/10.1145/2023582.2023585

[20] Jean Faugier and Mary Sargeant. 1997. Sampling hard to reach populations. *Journal of Advanced Nursing* 26, 4 (1997), 790–797. https://doi.org/10.1046/j.1365-2648.1997.00371.x arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2648.1997.00371.x

[21] Leonidas L Fragidis and Prodromos D Chatzoglou. 2018. Implementation of a nationwide electronic health record (EHR). *International journal of health care quality assurance* 31, 2 (March 2018), 116—130. https://doi.org/10.1108/ijhcqa-09-2016-0136

[22] Steven Furnell and Kerry-Lynn Thomson. 2009. Recognising and addressing 'security fatigue'. *Computer Fraud & Security* 2009, 11 (2009), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

[23] The Medical Futurist. 2019. Where Is Digital Health Heading In Denmark? https://medicalfuturist.com/danish-digital-health-strategy/

[24] Xiaocheng Ge, Richard F. Paige, and John A. McDermid. 2009. Domain Analysis on an Electronic Health Records System. In *Proceedings of the First International Workshop on Feature-Oriented Software Development (FOSD '09)*. Association for Computing Machinery, New York, NY, USA, 49–54. https://doi.org/10.1145/1629716.1629727

[25] Nathaniel S Good, Jens Grossklags, Deirdre K Mulligan, and Joseph A Konstan. 2007. Noticing notice: a large-scale experiment on the timing of software license agreements. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 607–616.

[26] Maren Sander Granlien and Morten Hertzum. 2009. Implementing New Ways of Working: Interventions and Their Effect on the Use of an Electronic Medication Record. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work (GROUP '09)*. Association for Computing Machinery, New York, NY, USA, 321–330. https://doi.org/10.1145/1531674.1531722

[27] Trisha Greenhalgh, Susan Hinder, Katja Stramer, Tanja Bratan, and Jill Russell. 2010. Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *BMJ* 341 (2010). https://doi.org/10.1136/bmj.c5814 arXiv:https://www.bmj.com/content/341/bmj.c5814.full.pdf

[28] HealthIT.gov. 2019. What are the differences between electronic medical records, electronic health records, and personal health records? https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal

[29] Ursula Holm. 2015. Ved du hvem, der har set dine sundhedsoplysninger? https://www.magasinethelse.dk/ved-du-hvem-der-har-set-dine-sundhedsoplysninger/

[30] Thomas Hupperich, Hans Löhr, Ahmad-Reza Sadeghi, and Marcel Winandy. 2012. Flexible Patient-Controlled Security for Electronic Health Records. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (IHI '12)*. Association for Computing Machinery, New York, NY, USA, 727–732. https://doi.org/10.1145/2110363.2110448

[31] Rick Kam and Posted By: Roberta Mullin. 2012. Electronic Health Records vs. Patient Privacy: Who Will Win? https://www.healthitanswers.net/electronic-health-records-vs-patient-privacy-who-will-win/

[32] Thomas Kostera and Cinthia Briseño. 2018. #SmartHealthSystems: Denmark and the national health portal. https://blog.der-digitale-patient.de/en/smarthealthsystems-denmark-national-health-portal/

[33] Annegerd Lerche Kristiansen. 2020. Mary Føler Sig Snydt: Deltog I Forsøg Til Gavn for Danske Kvinder – Blodprøver endte som forretningseventyr I USA. https://www.dr.dk/nyheder/webfeature/ssi

[34] laeger.dk. [n.d.]. Hårdere kurs mod uretmæssige opslag i journaler. https://www.laeger.dk/haardere-kurs-mod-uretmaessige-opslag-i-journaler

[35] Catherine Lim, Andrew Berry, Tad Hirsch, Andrea Hartzler, Edward Wagner, Evette Ludman, and James Ralston. 2016. "It just seems outside my health": How Patients with Chronic Conditions Perceive Communication Boundaries with Providers. *DIS. Designing Interactive Systems (Conference)* 2016. https://doi.org/10.1145/2901790.2901866

[36] Yves Longtin, Hugo Sax, Lucian L. Leape, Susan E. Sheridan, Liam Donaldson, and Didier Pittet. 2010. Patient Participation: Current Knowledge and Applicability to Patient Safety. *Mayo Clin Proc.* 85, 53–62. https://doi.org/10.4065/mcp.2009.0248

[37] Graham G Macdonald, Anne F Townsend, Paul Adam, Linda C Li, Sheila Kerr, Michael McDonald, and Catherine L Backman. 2018. eHealth Technologies, Multimorbidity, and the Office Visit: Qualitative Interview Study on the Perspectives of Physicians and Nurses. *J Med Internet Res* 20, 1 (26 Jan 2018), e31. https://doi.org/10.2196/jmir.8983

[38] Delfina Malandrino, Andrea Petta, Vittorio Scarano, Luigi Serra, Raffaele Spinelli, and Balachander Krishnamurthy. 2013. Privacy Awareness about Information Leakage: Who Knows What about Me?. In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society (WPES '13)*. Association for Computing Machinery, New York, NY, USA, 279–284. https://doi.org/10.1145/2517840.2517868

[39] Manisha Mantri, R. Rajamenakshi, and Gaur Sunder. 2019. Addressing data privacy in digital health: Discussion on policies, regulations, and technical standards in India. https://doi.org/10.5281/zenodo.3297267

[40] David Martin, Mark Rouncefield, Jacki O'Neill, Mark Hartswood, and Dave Randall. 2005. Timing in the Art of Integration: 'That's How the Bastille Got Stormed'. In *Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work (GROUP '05)*. Association for Computing Machinery, New York, NY, USA, 313–322. https://doi.org/10.1145/1099203.1099256

[41] Deven McGraw and Kenneth D. Mandl. 2021. Patient Participation: Current Knowledge and Applicability to Patient Safety. *NPJ Digit Med* 4. https://doi.org/10.1038/s41746-020-00362-8

[42] Alison R. Murphy. 2014. The Collaborative Management of Information Problems in Hospitals. In *Proceedings of the 18th International Conference on Supporting Group Work (GROUP '14)*. Association for Computing Machinery, New York, NY, USA, 263–265. https://doi.org/10.1145/2660398.2660436

[43] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, USA.

[44] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147.

[45] Irina Osovskaya. 2017. Personal Health Records: Understanding the Factors That Contribute to Creating Value and Practical Use by Patients and Citizens. In *Proceedings of the 2017 International Conference on Digital Health (DH '17)*. Association for Computing Machinery, New York, NY, USA, 237–238. https://doi.org/10.1145/3079452.3079484

[46] Stefanie Pötzsch. 2009. Privacy Awareness: A Means to Solve the Privacy Paradox?. In *The Future of Identity in the Information Society*, Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 226–236.

[47] Kristian Balle Ravn. 2016. Efter Kritik af Snageri I SUNDHEDSDATA: Sådan overvåger Du Adgangen til dine egne data. https://www.version2.dk/artikel/efter-kritik-snageri-sundhedsdata-saadan-overvaager-du-adgangen-dine-egne-data-979212

[48] Alsaleh Saad. 2019. The Influence of Users Privacy and Discomfort on Using Healthcare Information System. In *Proceedings of the 2019 the 5th International Conference on E-Society, e-Learning and e-Technologies (ICSLT 2019)*. Association for Computing Machinery, New York, NY, USA, 68–72. https://doi.org/10.1145/3312714.3312734

[49] Morten Schmidt, S. Schmidt, K. Adelborg, J. Sundbøll, K. Laugesen, V. Ehrenstein, and H. Sørensen. 2019. The Danish health care system and epidemiological research: from health care contacts to database records. *Clinical Epidemiology* 11 (2019), 563 – 591.

[50] Mikkel Secher. 2019. Ekssvigermor snagede I sygejournal - SÅDAN tjekker du, om NOGEN Har Kigget I din. https://nyheder.tv2.dk/samfund/2019-12-29-ekssvigermor-snagede-i-sygejournal-saadan-tjekker-du-om-nogen-har-kigget-i-din

[51] Pan Shi, Heng Xu, and Yunan Chen. 2013. Using Contextual Integrity to Examine Interpersonal Information Boundary on Social Network Sites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. Association for Computing Machinery, New York, NY, USA, 35–38. https://doi.org/10.1145/2470654.2470660

[52] H. Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35 (12 2011), 989–1015. https://doi.org/10.2307/41409970

[53] Tine Møller Sørensen and Gry Hoffmann. 2016. Hele skadestuen kan se OM du HAR KLAMYDIA. https://www.dr.dk/nyheder/indland/hele-skadestuen-kan-se-om-du-har-klamydia

[54] Anselm Strauss and Juliet Corbin. 1990. *Basics of qualitative research*. Sage.

[55] sundhed.dk. 2008. IT brings the Danish health sector together. https://www.medcom.dk/media/1175/it-brings-the-danish-health-sector-together_3.pdf

[56] sundhed.dk. 2015. Ved du, hvem der kigger i din journal og medicinoplysninger? https://www.sundhed.dk/borger/service/om-sundheddk/nyheder/ved-du-hvem-der-kigger-i-journal/

[57] sundhed.dk. 2018. Om din samtykkeerklæring. https://www.sundhed.dk/borger/service/hjaelp/om-portalen/datasikkerhed/din-egen-datasikkerhed/om-din-samtykkeerklaering/

[58] Gunnar Lind Haase Svendsen and Gert Tinggaard Svendsen. 2015. The Puzzle of the Scandinavian Welfare State and Social Trust. *Issues in Social Science* 3, 2 (2015), 90–99. https://doi.org/10.5296/iss.v3i2.8597

[59] thelocal. 2016. Five million Danish ID numbers sent to Chinese firm. https://www.thelocal.dk/20160720/five-million-danish-id-numbers-sent-to-chinese-firm-by-mistake/

[60] Michael Thykier. 2019. I hele landet snager personale i vores intime sundhedsoplysninger. https://politiken.dk/indland/art7567095/I-hele-landet-snager-personale-i-vores-intime-sundhedsoplysninger

[61] Thomas Trojer, Basel Katt, Thomas Schabetsberger, Ruth Breu, and Richard Mair. 2012. Considering Privacy and Effectiveness of Authorization Policies for Shared Electronic Health Records. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (IHI '12)*. Association for Computing Machinery, New York, NY, USA, 553–562. https://doi.org/10.1145/2110363.2110425

[62] version2. 2020. Uhindret adgang til 500.000 CPR-numre og Sundhedsdata i Region Syddanmark. https://www.version2.dk/artikel/uhindret-adgang-500000-cpr-numre-sundhedsdata-region-syddanmark-1089890

[63] Eric Wierda, Sebastiaan Blok, G Aernout Somsen, Enno T van der Velde, Igor I Tulevski, Borut Stavrov, Maud C C de Wildt, Bert J H van den Born, Laura Breukel, Bas A J M de Mol, M Corrette Ploem, and Michiel M Winter. 2020. Protecting patient privacy in digital health technology: the Dutch m-Health infrastructure of Hartwacht as a learning case. *BMJ Innovations* 6, 4 (2020), 170–176. https://doi.org/10.1136/bmjinnov-2019-000399 arXiv:https://innovations.bmj.com/content/6/4/170.full.pdf

[64] Pamela J. Wisniewski and Xinru Page. 2022. Privacy Theories and Frameworks. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer.

[65] Øivind Klungseth Zahlsen, Dag Svanæs, Arild Faxvaag, and Yngve Dahl. 2020. Understanding the Impact of Boundary Conditions on Participatory Activities.. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, Article 81, 11 pages. https://doi.org/10.1145/3419249.3420129

[66] Laura Zurita and Christian Nøhr. 2004. Patient opinion–EHR assessment from the users perspective. *Studies in health technology and informatics* 107, Pt 2 (2004), 1333—1336. http://europepmc.org/abstract/MED/15361031

Received July 2021; revised September 2021; accepted October 2021