Non-Static Nature of Patient Consent: Shifting Privacy Perspectives in Health Information Sharing

Aisling Ann O'Kane
UCL Interaction Centre
University College London
London, United Kingdom
a.okane@cs.ucl.ac.uk

Helena M. Mentis
Socio-Digital Systems
Microsoft Research
Cambridge, United Kingdom
hementis@microsoft.com

Eno Thereska
Systems and Networking
Microsoft Research
Cambridge, United Kingdom
etheres@microsoft.com

ABSTRACT

The purpose of the study is to explore how chronically ill patients and their specialized care network have viewed their personal medical information privacy and how it has impacted their perspectives of sharing their records with their network of healthcare providers and secondary use organizations. Diabetes patients and specialized diabetes medical care providers in Eastern England were interviewed about their sharing of medical information and their privacy concerns to inform a descriptive qualitative and exploratory thematic analysis. From the interview data, we see that diabetes patients shift their perceived privacy concerns and needs throughout their lifetime due to persistence of health data, changes in health, technology advances, and experience with technology that affect one's consent decisions. From these findings, we begin to take a translational research approach in critically examining current privacy enhancing technologies for secondary use consent management and motivate the further exploration of both temporally-sensitive privacy perspectives and new options in consent management that support shifting privacy concerns over one's lifetime.

Author Keywords
Privacy; temporality; medical records; chronic illness; illness trajectory.

ACM Classification Keywords
H.5.2 [Information Interfaces and Presentation]: User Interfaces - Interaction styles.

General Terms
Human Factors; Design; Measurement.

INTRODUCTION

The National Health System (NHS) in England offers lifetime medical services with an eye towards capturing detailed health records on a national scale for medical and public health research needs. This is motivated firstly by the purported benefits of sharing a patient's medical records between the healthcare providers that treat and care for that patient. However, the digitized and comprehensive nature of such medical records is also particularly supportive of the patient data needs of organizations (e.g. a hospital trust tracking mortality rates), national (e.g. disease tracking), and research agendas (e.g. treatment efficacy studies). In late 2011, approval was granted in the UK for health information to be made available to both industry and academic researchers [7, 23] through the Secondary Uses Service (SUS), a single, comprehensive repository for UK healthcare data [29]. In order to use collected data, though, patients must provide consent to secondary medical data use. Secondary use refers to the use of data for purposes other than it was initially collected for. In healthcare, this may include the transfer of a general practitioner's patient records into a national center's database for use in public health disease tracking or research on medication efficacy. Current guidelines in the UK provided by the General Medical Council [11] stipulate how to gain consent for particular data usage for research and the necessary security measures put into place (both in terms of policy as well as system design). This is in order to ensure the continued maintenance of patient privacy of their medical information that is transferred to the SUS for secondary medical data use [11].

However, medicine is temporal in nature [34] and perspectives on data sharing and privacy can change [19]. This raises questions as to how current perspectives on gaining consent and maintaining anonymity are temporally restrictive and could provide a hindrance in future medical and public health research, possibly breaching a patient's sense of privacy. Issues relating to the non-static nature of patient consent are particularly relevant for conditions that can last a lifetime, such as with chronic illnesses. This includes a particularly large swath of the population, as chronic illness conditions affect approximately half of all American and British adults – 133 million Americans and 17.5 million Britons [6, 48] – and these numbers are expected to continue to rise [43]. Chronic illnesses generally progress slowly with long durations [47] and thus some require a lifetime of on-going care and communication between the patient and their specialized

CSCW '13, February 23–27, 2013, San Antonio, Texas, USA.
Copyright 2013 ACM 978-1-4503-1331-5/13/02...$15.00.

healthcare providers, along with a lifetime of medical documentation [44].

An understanding of how patients regard the privacy of medical information they generate, share, and use to collaborate care is necessary to select mechanisms to securely and properly share health data in order to benefit medical research pursuits as well as ensure patient privacy and control over their data. Patient privacy, which includes the ability to exclude others from knowledge about one's health [19] is not an absolute right, as it has to be balanced with societal and other's rights in the healthcare domain [3]. However, confidentiality, including the respectful handling of disclosed personal knowledge in a trustful relationship [19], has traditionally been an essential part of healthcare worldwide [3]. Therefore, any understanding of patient privacy concerns and needs should be balanced with information and compliance needs of the patients' network of healthcare providers and the needs of those reliant on the SUS.

In the following exploration of perspectives on medical information privacy and sharing, we have focused on one particularly prevalent chronic health condition: diabetes. Through interviews with diabetic patients and diabetes health specialists on prior experiences with sharing health information, we have uncovered a clear trend that attitudes towards sharing sensitive health information had shifted due to factors such as changing concerns over the persistence of health data, health and lifestyle changes, technology advances, and technology experiences. Shifts can be towards the patient wanting to allow more or less of their health information to be shared with other parties than they had previously allowed. However, the occurrence of changes in one's privacy needs without the complimentary mechanisms of allowing a patient to change their prior consent exposes a gap in current consent management techniques.

Our interest in this question is in order to benefit a translational research agenda in design solutions for effective consent management systems and procedures and encourage further exploration of time sensitive privacy perspectives and technology solutions. After we present our findings on the non-static nature of patient privacy perspectives in sharing their health information, we turn our attention to a critical review of two current popular Privacy Enhancing Technologies (PETs). As an example of how it could be addressed, we then introduce a substantially different alternative that would require a shift in the collection and sharing of private health information (particularly for secondary uses) and a mechanism for achieving this system. Thus, our aim with this paper was to (1) bring the occurrence of shifting perceptions to light in order to stimulate a discussion within the CSCW health informatics community as well as (2) discuss the failure of current design mechanisms in addressing some of issues uncovered and how they could be addressed.

BACKGROUND

Studies exploring people's attitudes towards sharing medical information to inform research have hinted towards shifting perspectives and concerns over future data use being a factor in a patient's health data privacy preferences and perceptions. For instance, in one study of 1,230 Canadian adults in 2005, 56% reported an increased concern over their privacy in the previous five years [46]. A larger study of 4,659 US adults in 2007-2008 found that 37% worried that their DNA, medical information, and lifestyle information being collected and used in genetic research could be used against them in the future [16]. And a survey in 2008-2009 of 1,159 older (>64) US genomic research patients showed that 14% indicated that they would choose not to consent to sharing their information with a secondary database such as the National Genotypes and Phenotypes database due to concerns about future uses of the data [21]. Of course, privacy attitudes do not exist in a vacuum as they are "part of a larger social, cultural, political, and economic world" [35, p. 42]. In the UK in particular, attitudes towards privacy of health information have changed significantly as "unfettered access to personal health information is a thing of the past" [3, p. 725].

Although there are many factors that influence health information sharing concerns, changing perceptions of privacy are importance when considering the growing concern in many western countries over the management and tracking of chronic illnesses [6]. A chronic illness is one that can be controlled but not cured and therefore requires a lifetime of on-going, continually shifting care [33]. As a chronic illness can change and morph over time [20], the constant tracking of this information is of importance for a patient's own health records and trajectory as well as for public health monitoring [6]. This is in line with Strauss and Fagerhaugh's illness trajectory [40], which refers to the physiological unfolding of a patient's disease and the practices of care surrounding it over time, along with the claims of those in the CSCW community such as Reddy, Dourish and Pratt who argue that clinical information seeking and sharing is temporally coordinated [34] and Palen and Aaløkke who showed that a patient's home-based care is attuned to temporal rhythms [32].

A particular chronic illness of growing importance is that of diabetes. It affects the production of insulin, which is needed to process digested sugars, with Type I patients having no insulin production and Type II patients with deteriorated insulin production. The nature of diabetes means that onset could occur from childhood and last until late in life, making it a valuable context for studying the temporal nature of privacy attitudes. Type I is commonly associated with childhood onset and Type II with late adulthood, but this is not necessarily the case [17] and this is represented within our sample of patients. Diabetes is growing more prevalent every year, with estimates by the World Diabetes Association that one in ten will have the condition by 2030 worldwide [15]. Low glucose levels can lead to ill health effects immediately, but long-term excess levels of sugar can eventually lead to serious complications including eye, foot, kidney and heart disease. Both the maintenance of Type I and Type II diabetes require a range of treatments including diet, exercise, and medication, all of which need to be balanced by the patient to self-control their levels of ingested glucose [15]. There is no one-size-fits-all treatment plan for either diabetic condition; whether they are Type 1 or Type II, the patient must coordinate with their health providers to determine a sustainable health plan. To add to the complexity of care, the lifelong nature of these chronic conditions means that patients' health and lifestyles will change [30] along with the technology and treatments involved in their care [18].

As chronically ill patients have more experience with the transformation and use of temporally situated health data than the general patient population, the focus of this study was on how diabetes patients and caregivers have perceived their data sensitivity and privacy needs throughout their lifetime of care. Our findings show that the nature of a patient's illness trajectory and other temporally-situated outside influences can impact how patients perceive security and privacy concerns, ultimately impacting efforts in using shared health information for secondary uses.

METHODS

Research Setting

In this study, our focus was on the chronic condition of diabetes. The original intent was to study a group of patients affected by one chronic illness and although many patient groups were initially considered, a strategic decision was made early on in the study to focus on diabetes patients. Despite concerns over limits to the generalizability of eventual results, this proved to be a fruitful choice because of ease of access for the research team to this particular patient population.

This research was carried out in Eastern England, with support from local hospitals' diabetes service groups. The study centered on interviews of two important groups in a diabetic patient's care and information management: diabetic patients and diabetic specialists. Diabetic patients are people who have been diagnosed with Type I or Type II diabetes and are in charge of their own self-care (i.e. they are not a child, invalid, etc.). Diabetic specialists are those trained medical and health practitioners who specialize in diabetic care.

Sampling Procedure

The study used a theoretical, non-probabilistic sampling procedure [22]. Interviews with diabetes patients were first conducted in person with patients known personally to the researchers. We then conducted further patient interviews by telephone with diabetes patients recruited from the UK Internet board Gumtree, a weekly student union news email to a local university's undergraduate population, local diabetes support groups, physical advertisements in grocery stores around Eastern England, and directly emailing three popular diabetes patient bloggers. In addition, we conducted a group interview with a diabetes support group in the Greater London area. This ensured a wide range of interviewees with varied experiences and backgrounds, including those with Type I diabetes since childhood, two men with Type I diabetes onset in their early thirties and forties, elderly Type II patients, and a late twenties male with Type II diabetes. Each of these interviewees was rewarded with a £10 or $15 Amazon gift certificate. Demographics are in Table 1.

Gender	
Male	15
Female	12
Age (year range 18-73)	
<30	5
30-50	8
>50	14
Years Since Diagnosis (year range 2-32)	
1-5	5
6-10	4
11-15	7
>15	11
Diabetes Type	
TI	12
TII	15
Comfort With Technology	
Very	11
Somewhat	13
Not	3
Interview Source	
Group Interview	12
Support Group Follow-up Contact	2
UK Internet Board Gumtree Advertisement	1
University Newsletter Advertisement	2
Grocery Store Advertisement	5
Personally Known to the Researchers	2
Contacted by Email (Bloggers)	3

Table 1. Diabetes Patient Participant Demographics (N=27)

In interviewing diabetes specialists, convenience sampling was used. We interviewed six UK based diabetes health specialists: two senior diabetes consultants, a diabetes midwife, a diabetes nurse, a diabetes podiatrist, and a diabetes dietician. They were recruited from diabetes services groups in two hospitals in Eastern England through the head of one of the services groups. The interviews were conducted by phone except for the diabetes nurse and first consultant, who were interviewed at their hospital in person. Each interview concluded when the interviewer felt a clear picture of the participant's perspectives on medical information sharing and privacy experiences were covered. Each interview was at least 30 minutes.

Data Collection Procedure

The interviews, including the group interview, were conducted by the first author and audio recorded for all sessions. These recordings were transcribed verbatim and the qualitative research software Atlas Ti was used to manage the dataset. All interviews were conducted in a semi-structured format with interview questions probing people's experiences with their medical information exchange networks as well as their attitudes towards it.

Topic	Questions
Experience with the condition	Could you describe how it affects a diabetes patient's day? Is there anything about diabetes that makes it unique from other conditions?
Online information use	Have you used any online diabetes health resources? Have you ever used Twitter or Facebook for diabetes information? Do you read blogs and forums for diabetes information?
Medical information use	What kinds of documents are used for diabetes care? Have you used electronic medical records before? What kinds of documents are shared?
Accessing medical information	Who should have full access to medical records? Who should have partial access to medical records? Who should decide who has access?
Expectations for medical information	When do you expect a new caregiver to first have access to a medical record? For how long do you expect a caregiver to have access to your medical record?
Changing medical information	Who do you think should have the right to modify portions of a health record? Over time, should some information be withheld or retired from access?
Sharing medical information	Have you ever encountered any issues with privacy and health records? What are your views on privacy and online health documents? Do you have any concerns with the shift from paper to electronic records?

Table 2. Interview and Group Interview Questions

Similar questions were asked of the two user groups with changes to the language based on the participant, as seen in Table 2. During these interviews, patients reflected on their current privacy concerns, prior experienced privacy breaches, and concerns about future privacy issues.

Data Analysis

A descriptive, exploratory research approach such as thematic analysis is well suited to uncover the nature of privacy concerns for chronically ill patients. Thematic analysis was chosen to systematically analyze the data whilst also allowing us to tap into latent themes that manifested in the data collected [1], going beyond observations to more tacit themes [24]. Subsequent integration of these latent themes with the researchers' interpretation of the literature uncovered the need for further studies to explore the realities of the changing perceptions of and attitudes towards one's health information privacy. The emergent themes formed the basis for the introduction of a mechanism that supports the temporally sensitive perspectives on privacy [9].

Thematic analysis was conducted using an open, iterative coding scheme on the qualitative data collected from the interviews conducted [1]. A three-step approach was used for coding the data. Coding was organized first around the broad theme of 'shifts'. The evidence that attitudes towards privacy are not consistent led to further classifying the qualitative data by changes in technology, changes in health, and changes in lifestyle. Finally, this coding allowed deeper analysis into the changing perspectives of the patients and specialists around the sharing and use of sensitive medical information. The study's findings were assessed through an evaluation of validity and reliability by ensuring that we included patients with variation in diabetes experiences, triangulation of data collection and analysis methods (interviews and group interview), and through the relationship to prior literature [12].

RESULTS

Solutions for instituting protection for patient health information privacy tend to address one's privacy attitudes as a static state: that a successful model of privacy need only be concerned with the proper anonymisation after consent has been gained from a patient [32, 41, 42]. However, because this study's focus is specifically on how and why a patient's perceptions of privacy can shift and change, four related but different themes emerge from the data that encompass the shifting nature of privacy perceptions: concerns over the persistence of health data, health changes, technology advances, and technology experiences.

Persistence of Health Data and Its Changing Relevance

Despite the political and technological push towards the collection of a lifetime of digitized health records, we found that a predominant concern of diabetes patients who have a lifetime of health records in relation to their chronic illness is the perseverance of health information. Their concern in keeping much of the information that was previously recorded private, is primarily due to patients' interest in maintaining their dignity and privacy, which can outweigh their interest in their health [4]. For instance, one's indiscretions when young can be deemed private information to a recently diagnosed, middle aged, Type II diabetic. Although a patient may provide consent for data to be accessible to others at one time, this does not mean that in ten years patients might not want to hide such data. Likewise, if the collection of current data also requires the collection of previous data, the relevancy of this need may not be immediately obvious to a patient [39]. This is because, oftentimes, previous health and behavior is a contributing factor to current health issues and behavior. Thus, many things could be relevant or could lead researchers to ascertain a relationship between seemingly disparate data.

> The things that happened in the past often are still affecting the patient in the future. Let's say they've been anorexic or something. It may get deleted from the record and you don't know. You wonder why they're not eating properly and not wanting to see a dietician and not taking care of themselves. – *Podiatrist*

However, patients do not realize this information is what specialists and researchers need to know. When asked to share such personal, sensitive, and seemingly irrelevant information, the first reaction of many patients is of distrust. Moreover, if another party was privy to that information, then anger can ensue.

> They had gotten information that had nothing to do with anything really and I felt that that was inappropriate and too personal. Yeah, you know the podiatrist again, just qualified, knows nothing about me, doesn't know anything but I've got corns, why should they know […] that my diabetes was out of control when I was 18? […] It's got to be relevant, surely. *– Patient 3*

Patients do not always understand the complex interrelated workings of their health [2]. Thus many of our patient interviewees wished to have a greater discussion over what is and what is not relevant in their records. However, in situations such as these, it was not clear as to who should decide relevancy while also being cognizant of patient trepidation of the persistence and distribution of prior data.

> I suppose there are always going to be plenty of things which have ceased to be relevant but somebody somewhere has got to make a decision about these and I would feel that the making of the decision of which records to expunge is probably taking up time which any professional will have in short supply and might be – might want to use in a more effective way. *– Patient 11*

This is an important question as even healthcare practitioners are not omniscient in knowing what data will and will not be relevant. For example, it was not that long ago that the link between a diet high in refined carbohydrates was linked to a greater risk of Type II diabetes [14]. Some participants understand that when more information is made available, the better it is for their own healthcare as well as for research. But the requirement for privacy is even greater as increasingly sensitive information is being shared with unknown third parties.

> If health professionals are looking at your health records, they want to see the whole picture. … And if they suddenly discover that there is a certain trend or suspect or do research on the fact that there is a certain trend in diabetes or whatever condition you have actually got… Say for example the fact that you smoked when you were 20, if you want to take that piece of information out of your records they are not going to be able to find it, so I don't think it actually helps treatments longer term, so I would say no, I think your records should stay even if there is stuff there that you would like to be taken off. – *Patient 8*

> I think there's a lot of people who care that 'what if I don't want them to know this about me?' It doesn't matter. They need to know everything that's going on in your health. If you had an STD or if you're on a certain kind of medication, a certain doctor still needs to know about that. *– Patient 15*

As one's behavior changes, one's perception of the sensitivity of previously recorded and shared data may change as well. However, retroactively removing previously recorded data that at the time was considered acceptable, but now the patient perceives it as sensitive, is not a possibility.

Health Changes Influence Privacy Attitudes

As a chronic condition such as diabetes changes over time, the nature of a person's condition can also change their views on their health information privacy. Although some people might be open to sharing information on their diabetes, if the associated effects of the illness changed or if a person was afflicted with something else in addition to diabetes, they become more or less private about their health information, such as with sharing information about a stigmatized illness [45]. In our interviews, the majority of patients acknowledged the way they share information, whether it be with family members or online, may change based on his or her condition.

> I'm out there blogging and sharing my life with diabetes with my real name and my picture and stuff like that, so I consider my diabetes world kind of an open book. But there are other people who I definitely think would be very concerned about the privacy of their health records. Now if it were to cross over into health issues that maybe were not diabetes related, I think I would feel a little differently about that. *– Patient 13*

The open sharing behavior and privacy attitudes of the diabetes patients we interviewed differs from the behavior and attitudes of other chronically ill patients, perhaps with stigmatized illnesses such as mood disorders and HIV [45].

These health changes would be beneficial to capture in a medical record that could inform large-scale medical data aggregation, but this might not always be preferable to patients as new health scenarios could bring about different attitudes.

> Well privacy is an interesting thing, right. A scenario could change very quickly, and I could easily see myself being more concerned with the privacy aspect of it than the control. *– Patient 13*

Beyond changes in the nature of a patient's medical health, it cannot be assumed that the way he or she values privacy will be consistent while dealing with a chronic condition that could last their lifetime. New responsibilities, such as having children who manifest a chronic illness, cause people to alter their perceptions of the privacy of their own health data and the importance of medical research purposes, while on the other hand, responsibilities may diminish as complications arise in older diabetics. Patient 9 developed cancer and required an arm amputation causing a lifestyle change that required him to rely on his wife to handle his health documentation. Subsequently, he expressed a reduction in anxiety when asked about his views on the privacy of his medical records.

> I am not really bothered. I am happy I should be told what I want to know and they should do what they need to do… Because I do get help so it doesn't bother me. My wife does most of the computer work…I don't do much since I lost my arm. – *Patient 9*

Thus, a change in health itself can change one's perspective of privacy. On the one hand, the onset of new illnesses, such as a mental illness, may cause a once open patient to want to be more private about their information whereas other health onsets cause one to loosen their perspective on privacy as we see with the patient who lost his arm and had already given up autonomy to his wife.

Technology Advances Lead to Greater Perceived Privacy Risks

As time passes, new types of medical care options are available for diabetes patients through innovations in medical research and technologies [8]. These advances can lead to changes in the way patients want to share their health information and their attitudes towards privacy. With the move to networked electronic medical records, patients that may be currently very comfortable with technology believe there is potential for additional security issues and worry more about privacy, as per the Canadian study mentioned in the Background [46].

> I mean banks can get hacked, I care about my money, but I do care about my health more. So I would rather... it's just the security of that information. I mean if they're online, people having access to things that they shouldn't have access to, I don't know. It makes me nervous though I understand the necessity of it, but it does make me a little nervous. *– Patient 14*

These increased privacy concerns are not necessarily justified based on the technology change, but are linked with other factors such as patients' previous exposure to technology in general [31]. Issues with privacy are perceived to be more important as they are more noticeable or more easily captured with new technology compared to previous solutions, such as the security concerns surrounding paper receiving far less attention than its digital equivalent [5]. Evidence of this is highlighted in stories of security breaches that have occurred with both electronic and paper health records.

> Well we have had some instances in the [hospital] that we've had to take action when people have accessed records inappropriately. The interesting thing about that is, had there been paper records, we would have never been able to prove it or sort it out. *– Consultant 2*

When patients are not familiar with these new systems or have little experience with newer technologies, they can be wary of them [31]. This is seen through technology advances such as new glucometers or insulin pumps bringing up brand new privacy concerns for diabetes patients.

> Actually I had one patient the other day email me about, her husband worked for IT, and had found this article about how insulin pumps can be interfered with and overdose you with your insulin, and certain companies can kind of…I'm not sure where it really came from, but obviously I directed her to that company to bring it up with them. – *Diabetic Nurse*

Technology innovations that patients and care providers have already experienced have been shown to affect their views towards the privacy of their medical records. Technical innovations as well as the shift towards EMRs show that patients are wary of what this means for the security of their information. As new information and news stories emerge, they can lead to a patient changing his or her mind regarding privacy needs. One may want to revoke their consent in having their information listed in a repository, such as the SUS. Although all stakeholders recognize there is great potential in the collection of this information for medical research, the patients will have concerns that may or may not be well founded based on their knowledge of new technologies.

Technology Experience Leads to Fewer Privacy Concerns

Newfound worries changed patients' perception of the risks to their privacy yet there is no mechanism to revoke the agreements they made in the past. However, although the access to new technologies brings up new privacy concerns for patients, they are increasingly sharing sensitive health information through another technology: the Internet and specifically social media. Patients are going online to aid in their own care, often facilitated by sharing with a large online community [13]. This acts as social and emotional support, which can be very important in caring for a chronic condition that can be "unrelenting". Diabetes patients use social media as "social support".

> [Its popularity] comes from openly sharing our vulnerabilities and some of our fears and sharing our hard times as well as our good times - *Patient 13*

> Just that it is extremely supportive and there's a huge value to people, to being surrounded by people who understand and who are like you. This community has grown at such a rate I think because there was a net organic need for it, and intrinsic need for it. – *Patient 14*

This is a massive shift in patients' care that is growing as this type of social support treatment is becoming easier to access [10]. The use of social media seems to be a fine balance between openly sharing sensitive medical information whilst also remaining in control of what is considered private.

> If you want to talk about the worst thing that you've done to your diabetes, or you are really ignoring it, or you're in a dark place, you can share that information without sharing your name, without alerting your employer to your potential issue or alerting your family even. You can keep those feeling private but share them publicly in a way gets the support without putting you out there like you're waving a flag saying 'I'm diabetic and I want everyone to look at me!' right? – *Patient 14*

Apart from health information, people are increasingly sharing sensitive information through social media [25]. The growing popularity of social media for medical knowledge and social support is changing people's perspectives as to what is private and what is not private, based on how vulnerable they feel. In these cases, people may choose to view previously held privacy beliefs as overly cautious and want to reveal more about their previous medical history, but they still have their own individual levels of comfort. Although Patient 13 would write his diabetes blog under his own name and picture as mentioned above, one group interview participant did not feel comfortable with this level of privacy.

> I think it would be alright to share information about how your, maybe how your blood sugars go…[…] but I don't think it is necessary to say your name and your address or anything like that. You can have a blog where everyone has a user name or something. And then I think it's really helpful. I don't think you really need to identify yourself. – *Group Interview Participant*

The benefit of easy to obtain information and social support over the Internet has increased the amount of sensitive medical information patients share, albeit not for the purposes of, say, aggregating large-scale medical data but rather for engaging with the 'Diabetes Online Community' [13]. Because they personally benefit from shared information and are able to directly see others benefit from their own medical information, patients seem to be happy to share sensitive healthcare details and employ their own tactics to keep their personal data anonymous. They have the control to reveal or hide information, revoke access to old posts, or open access up to all new content.

DISCUSSION

Due to the persistence of health data, changes in health, technology vulnerability, and technology experience, a patient's privacy attitudes can change over their lifetime. This lends evidence to the ever-changing notion of privacy and the consideration of mechanisms to allow for changes in privacy preferences to be accommodated. In the aim to start the discussion around addressing temporally-sensitive patient privacy in secondary medical data use in England, we turn our attention to two common, but surprisingly ineffective Privacy Enhancing Technologies (PETs). Then we describe a new mechanism that relies on zero-knowledge cryptographic proofs.

A Critical View of Current PET Mechanisms

Two popular mechanisms for PET support some of the issues we have outlined from our study: sealed envelope and pseudonymisation. Both of these have been considered in the design of the NHS health database [28, 26]; however, our discussion of these two mechanisms highlights how they are inadequate in addressing the privacy needs of patients over their lifetime as various circumstances shift their perspectives.

A 'sealed envelope' is a concept that provides security around parts of a shared electronic record to which a patient wishes to restrict access [28]. A wish may be expressed, for example, that sensitive information can be accessed by a patient's mental health practitioner, but not shared with a national health registry. If another health practitioner or public health researcher believes the sealed information to be important for their uses, they may request access to the information from the patient to 'un-seal the envelope'. Although sealed envelopes support the loosening of privacy perspectives due to either a change in circumstances or growing need to contribute to research, sealed envelopes do not support one's tightening of privacy perspectives due to concerns over new technologies or previously disclosed health data. In other words, although a retrospectively sealed envelope prevents future access, it does not remove data from SUS.

There has also been a strong movement towards protecting the identity of a patient through anonymisation; i.e., removing all identifying data of a patient. The problem with anonymisation is that it is a permanent process and once anonymised, it is not possible to link the data back to a particular individual. This may not always be acceptable, as a researcher may need to know that the patient who engaged in heavy drinking as a youth is the same patient who was diagnosed with diabetes at a later date. The mechanism of pseudonymisation, sometimes described as "reversible anonymisation" provides a solution [26, 27]. In effect substituting true patient identifiers with pseudonyms where the true identities are retained in a secure part of the information system allowing the relationship between old and new data to manifest. However, again, this mechanism does not support one's tightening of privacy perspectives as once consent is given, data is copied as a permanent part of the SUS and pseudonymised which again conflicts with our findings regarding concerns over new technologies or previously disclosed health data.

Thus, just as these two popular mechanisms show, the focus of PETs has been on the secure provision of medical information to secondary sources and, once provided, the assurance of anonymity [26-28]. However, this focus is missing the need to remove medical information from secondary repositories such as SUS and support the retroactive tightening of privacy settings for health care information.

A Fresh Take on Privacy Enhancing Technologies

Another option is potentially more supportive of temporally sensitive privacy. It was developed in the context of privacy-preserving smart metering [36] where a household's privacy may be threatened by allowing the electricity provider to access fine-grained electricity consumption data, from which privacy-sensitive user behavior in a household could be deduced. The intuition behind the solution is that metering and data aggregation does not have to happen at the electricity provider, but can happen at the households. The electricity provider would provide each household with a function to run over the user's electricity data, which guarantees privacy since the provider does not gather the household's data.

So, how would this model apply to the NHS and SUS? In England, the NHS has moved to a networked system model [38]. Although the initial plan was a centralized repository, this failed in its implementation; thus, now a distributed model is being used where all patient data is to be stored at the patient's general practitioner (GP). This same model can be used for secondary uses. First, the medical data always resides with the GP and is not stored elsewhere. Second, in many cases the researcher could create hypotheses to be run on the GP networked systems without having to look at the fine-grained user data. This allows the medical information to stay at the place of origin – the GP – thus allowing for changes requested by patients, perhaps based on changing privacy attitudes, to be fulfilled at their local GP's office. This would support the loosening and tightening of privacy expectations by patients as they can make these changes at the local GP's office, alleviating some of the concerns found in this study.

There are several technical challenges with this approach. First, there is a bootstrapping process that requires all devices onto which data is held to provide a proof that the original data has not been tampered with by the user. This bootstrapping phase will require GP systems capable of some basic cryptographic capabilities. There is evidence that these capabilities are minimal and current system architectures support them [36]. In addition, the medical community might not readily accept the proposed design as it ultimately calls for the data to be stored with the GP and not with the SUS. This decentralized architecture will have to allow privacy-preserving statistical aggregation of data to be transmitted to the researchers to support medical studies.

Limitations of the Current Study

Because the ultimate goal of mechanisms for privacy of medical data in secondary use is to uncover relationships and trends that can positively affect public health, having rich narrative data explicating the patient's perspective of privacy is both crucial and necessary. Nevertheless, the research agenda must go further to validate the concepts we have generated through further studies of other patients with diabetes, as well as other groups of chronically ill patients, and even people unaffected by a chronic illness. In addition, a longitudinal study of patients' actual changes in health information sensitivities would be helpful to compare to their recalled previous experience and envisaged future changes in privacy perceptions. It is hoped that the emergent concept of temporally situated patient privacy perspectives can then be applied in a more structured manner to guide the formative evaluation of secondary data use systems to empower patients toward greater participation in health reporting.

CONCLUSION

A chronic condition can affect a person from their childhood to late in life, and when one ponders the massive changes that can occur over lifetime, it is naïve to assume that the privacy concerns and the willingness to share health information will be anything close to consistent or static. Change in one's experience with technology and the nature of one's lifestyle or condition will influence one's willingness not only to share information that will be collected in a medical record but also how likely one will be to share information for the purpose of large scale medical data aggregation. A one-time consent management system would not respect the patients' wishes in the long-term so future systems should be able to adapt to changing attitudes that include both tightening and loosening of privacy sensitivities. Designers of these medical information systems supportive of large-scale medical data aggregation should be mindful of these implications and what this might mean for the quality of the data in these systems.

REFERENCES

1. Braun, V. and Clarke, V. Using thematic analysis in psychology. *Qualitative Research in Psychology 3*, 2 (2006), 77-101.
2. Bridson, J., Hammond, C., Leach, A. and Chester, M.R. Making consent patient centred. *British Medical Jour. 327*, 7424 (2003), 1159-1161.
3. Chalmers, J. and Muir, R.. Patient privacy and confidentiality. *British Medical Jour 326***,** (2003), 725-726.
4. Chochinov, H.M. Dignity and the essence of medicine: The A, B, C, and D of dignity conserving care. *British Medical Jour 335* (2007), 184.
5. Cleeff, A., Dimkov, T., Pieters, W. and Wieringa, R. Realizing Security Requirements with Physical Properties: A Case Study on Paper Voting. In *Proc. IT Convergence and Security 2011*. Springer Netherlands (2012), 51-67.
6. Department of Health. Improving Chronic Disease Management. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4075214.
7. Department of Health. Newly available Health Data will support Medical Research and Patient Empowerment. http://mediacentre.dh.gov.uk/2011/11/29/newly-available-health-data-will-support-medical-research-and-patient-empowerment/.
8. Diabetes UK. Current Research. http://www.diabetes.org.uk/Research/Current-research/.
9. Forsythe, D.E. Using ethnography to build a working system: rethinking basic design assumptions. In *Proc. Computer Applications in Medical Care 1992*. McGraw-Hill (1992), 510–514.
10. Fox, S., and Jones, S. The social life of health information. *Pew Internet*. www.pewinternet.org/Reports/2009/8-The-Social-Life-of-Health-Information.aspx.
11. General Medical Council Standards. Confidentiality guidance: Research and other secondary uses. http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_40_50_research_and_secondary_issues.asp.
12. Golafshani, N. Understanding reliability and validity in qualitative research. *The Qualitative Report 8,* 4 (2003), 597-607.
13. Greene, J.A., Choudhry, N.K., Kilabuk, E. and Shrank, W.H. Online social networking by patients with diabetes: a qualitative evaluation of communication with Facebook. *Jour. General Internal Medicine 26*, 3 (2011), 287-292.
14. Gross, L.S., Li, L., Ford, E.S. and Liu, S. Increased consumption of refined carbohydrates and the epidemic of type 2 diabetes in the United States: an ecologic assessment. *American Jour. of Clinical Nutrition 79*, 5 (2004), 774-779.
15. International Diabetes Federation. One Adult in Ten Will Have Diabetes by 2030. http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4075213.pdf.
16. Kaufman, D.J., Murphy-Bollinger, J., Scott, J. and Hudson, K.L. Public opinion about the importance of privacy in biobank research. *American Jour. of Human Genetics 85*, 5 20(2009), 643-54.
17. Kaufman, F.R. Type 2 diabetes mellitus in children and youth: a new epidemic. *Jour. of Pediatric Endocrinology and Metabolism*, *15*, Supplement (2011), 737-744.
18. Koro, C.E., Bowlin, S.J., Bourgeois, N. and Fedder, D.O. Glycemic control from 1988 to 2000 among US adults diagnosed with type 2 diabetes. *Diabetes Care 27*, 1 (2004),17-20.
19. Lowrance, W.W. Learning from experience. *Privacy and the seconda3ry use of data in health research.* Nuffield Trust (2002).
20. Lubkin, I.M. NS Larsen, P.D. *Chronic illness: Impact and interventions*. Jones & Bartlett Learning (2006).
21. Ludman, E.J., Fullerton, S.M., Spangler, L., Trinidad, S.B., Fujii, M.M., Jarvik, G.P., Larson, E.B. and Burke, W. Glad you asked: participants' opinions of re-consent for dbGap data submission. *Jour. Empirical Research on Human Research Ethics 5*, 3 (2010), 9-16.
22. Mays, N. and Pope, C. Qualitative research: rigour and qualitative research. *British Medical Jour 311*, 6997 (1995), 109.
23. Medical Research Council. e-Health Informatics Research – Securing the UK as a world leader. http://www.mrc.ac.uk/Ourresearch/ResearchInitiatives/E-HealthInformaticsResearch/index.htm.
24. Merton, R.K. Thematic Analysis in Science: Notes on Holton. *Science 188*, 4186 (1975), 335-338.
25. Narayanan, A. and Shmatikov, V. De-anonymizing social networks. In *Proc. Security and Privacy 2009*. IEEE (2009),173-187.
26. National Health Service. Pseudonymisation Implementation Project.

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo.

27. National Health Service. Pseudonymisation Implementation Project (PIP): Implementation Guidance on Local NHS Data Usage and Governance for Secondary Uses. http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/impguide.pdf.

28. National Health Service. "Sealed Envelopes" Briefing Paper: "Selective Alerting" Approach. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/confidentiality/sealedpaper.pdf.

29. National Health Service. Secondary Uses Service (SUS). http://www.ic.nhs.uk/services/secondary-uses-service-sus.

30. Nied, R.J. and Franklin, B. Promoting and prescribing exercise for the elderly. *American Family Physician 65*, 3 (2002), 419-430.

31. Or, C.K.L. and Karsh, B.T. A systematic review of patient acceptance of consumer health information technology. *Jour. of the American Medical Informatics Association 16*, 4 (2009), 550-560.

32. Palen, L. and Aaløkke. Of pill boxes and piano benches: Home-made methods for managing medication. In *Proc. of CSCW 2006*, ACM Press (2006), pp. 79-88.

33. Paterson, B.L. The shifting perspectives model of chronic illness. *Jour. of Nursing Scholarship 33*, 1 (2001), 21-26.

34. Reddy, M.C., Dourish, P. and Pratt, W. Temporality in medical work: Time also matters. *Computer Supported Cooperative Work 15*, 1 (2006) 29-53.

35. Regan, P.M. *Legislating privacy: Technology, social values, and public policy*, University of North Carolina Press (1995).

36. Rial, A. and Danezis, G. Privacy-preserving smart metering. In *Proc. Workshop on Privacy in the Electronic Society 2011*, ACM (2011), 49-60.

37. Rind, D.M., Kohane, I.S., Szolovits, P., Safran, C., Chueh, H.C. and Barnett, G.O. Maintaining the confidentiality of medical records shared over the Internet and World Wide Web. *Annals Internal Medicine 127*, 2 (1997), 138–141.

38. Robertson, A., Cresswell, K., Takian, A., Petrakaki, D., Crowe, S., Cornford, T., Barber, N., Avery, A., Fernando, B., Jacklin, A., Prescott, R., Klecun, E., Paton, J. Lichtner, V., Quinn, C., Ali, M., Morrison, Z., Jani, Y., Waring, J., Marsden, K. and Sheikh, A. Implementation and adoption of nationwide electronic health records in secondary care in England: qualitative analysis of interim results from a prospective national evaluation. *British Medical Jour 341*, (2010).

39. Roter, D.L. and Hall, J.A. Physicians' interviewing styles and medical information obtained from patients. *Jour. General Internal Medicine 2*, 5 (1987), 325-329.

40. Strauss, A.L. and Fagerhaugh, S. *Social organization of medical work*. Transaction Publishers (1997).

41. Sweeney, L. Guaranteeing anonymity when sharing medical data: the Datafly system. In *Proc. AMIA Annual Fall Symposium 1997*, PubMed Central (1997), 51–55.

42. Sweeney, L. Replacing personally-identifying information in medical records: the SCRUB system. In *Proc. AMIA Annual Fall Symposium 1996*, PubMed Central (1997), 333–7.

43. Tunstall-Pedoe, H. Preventing Chronic Diseases. A Vital Investment: WHO Global Report. *Jour. Epidemiology 35*, 4 (2006), 1107.

44. Wagner, E.H., Austin, B.T., Davis, C., Hindmarsh, M., Schaefer, J. and Bonomi, A. Improving Chronic Illness Care: Translating Evidence Into Action. *Health Affairs 20,* 6 (2001), 64-78.

45. Wicks, P., Massagli, M., Frost, J., Brownstein, C., Okun, S., Vaughan, T., Bradley, R. and Heywood, J. Sharing health data for better outcomes on PatientsLikeMe. *Jour. Medical Internet Research 12*, 2 (2010).

46. Willison, D.J., Schwartz, L., Abelson, J., Charles, C., Swinton, M., Northrup, D. and Thabane, L. Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public? *Jour. American Medical Informatics Association 14*, 6 (2007), 706-712.

47. World Health Organization. Chronic diseases. http://www.who.int/topics/chronic_diseases/en/.

48. Wu, S. and Green, A. Projection of chronic illness prevalence and cost inflation. RAND Health (2000).