“We should not do this, but we use WhatsApp”
Exploring Patient Data Exchange between Healthcare Professionals

Simon Anell
CISPA Helmholtz Center for Information Security

Francisco Nunes
Fraunhofer Portugal AICOS

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Abstract

Health-related sensitive patient data poses significant privacy challenges as it is essential for treatment and, therefore, often needs to be shared between different parties. In the course of this research project, we sought to understand 1) how sensitive data of chronic patients is handled by pharmacists and physicians, 2) which processes the two groups use to interact with patient data, and 3) where privacy-related problems occur. This can help us to understand the challenges of currently used systems and is essential to inform the design of future solutions. To answer our research questions, we conducted a qualitative study with pharmacists and physicians. We consulted with researchers and designers of healthcare systems and discussed with security and privacy researchers to inform our study. Among other findings, we found that participants are not only using existing and established healthcare systems, but also other means for communicating patient data, e.g., standard short messaging services to discuss cases more quickly and efficiently, and also to navigate around existing privacy laws and guidelines that they are aware of. Furthermore, we found that requirements identified by health professionals for sharing patient health data privacy-preserving and efficiently are hard to reconcile.

1 Introduction

Health-related, sensitive patient data poses significant privacy challenges as it is essential for therapy and, therefore, often needs to be shared between different parties. In the course of this research project, we seek to understand 1) how this sensitive data of chronic patients are handled by pharmacists and physicians, 2) which processes the two groups use to interact with patient data, and 3) where privacy-related problems occur. This will help us understand the challenges of currently used systems and is essential to inform the design of future solutions. We present a qualitative study with three pharmacists and two physicians that was informed by sessions with two designers of healthcare systems and two security and privacy researchers. Both pharmacists and physicians need access to patient health data, generate patient health data, and have contact with the patient - in the case of chronic care, regularly and over a long period of time. Among other findings of this work, we found that participants, next to existing and established healthcare systems, are using other means for communicating patient data, e.g., standard short messaging services to discuss cases more quickly and efficiently and also to navigate around existing privacy laws.

2 Methodology

To better understand data sharing among physicians and pharmacists, we conducted a qualitative user study that focuses on these two groups, focusing on exploring health professionals’ privacy perceptions when handling patient data. We decided on a co-design approach that we implemented with participatory design sessions, both with groups and individuals. We used digital whiteboards as a tool to facilitate our sessions. Participatory Design is a good approach to having interactive sessions with multiple users, participants can interact with each other, and topics can be discussed. Due to the challenge of recruiting multiple participants for one session, we also conducted single, interview-like sessions that would follow the same structure but would be adjusted to suit an interviewer-participant ratio of one to one.

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

Study Design and Session Structure

We designed a co-design user study with a scenario-based narrative with the utilization of an online digital whiteboard tool, Mural boards [1]. The study was divided into 7 Tasks: (1) Warmup and Introduction, (2) Professional Communication, (3) Discussion of 5 different data sharing and access Scenarios

The scenarios were the centerpiece of the study. They differed in the actors involved, the type of data shared, the medium used to share and store data, and the severity of the actions of the involved actors. For each scenario task, we explained the scenario and asked the participants (1) if they see privacy issues for any actor, (2) if they see advantages or disadvantages compared to processes they would use to handle the situations, and (3) if they would change some element in the interaction.

Analysis

One researcher coded the data under the supervision of a second researcher using thematic analysis. We used open coding and axial coding to analyze the data. We came up with two codebooks.

Ethical considerations

The participants were aware of the start and the end of data collection. They were informed several times that participation in the study was voluntary and that they could withdraw at any point without stating any reason and demand the deletion of their data. We clarified that the participants were not being tested and that there were no wrong answers.

3 Results

We conducted six Co-Design sessions with nine participants. Participants were German (6, 5 female) and Portuguese (3, 2 female). We recruited personal contacts, used email lists, and directly contacted pharmacies and doctor's offices.

Demands for an Electronic Health System: Access and Data Integrity: Patient data should be stored consistently and centralized for healthcare actors from different fields and institutions
Functionality: Automatic pre-diagnose functionality as well as notifications, could assist Healthcare professionals
Accessibility: Solutions always have to consider non-tech-savvy patients and have a fast fallback mechanism for urgent cases
Patient Burden: Patients' willingness to follow the treatment plan is essential for an efficient treatment. Therefore, the burden for patients should be as low as possible.

Perspectives on Data Sharing: Patient consent: Informed patient consent was mentioned as a prerequisite for sharing data between healthcare actors. If patient consent is given, sharing and processing data between medical professionals would not be an issue.
Media: Participants also mentioned the use of insecure media (Fax) and instant messengers for professional communication (e.g., WhatsApp) while acknowledging that these media might not be recommended or secure to use for patient data exchange.
Access vs. Modification and Information level: Other challenges that emerged were the distribution of read/write access rights and the implementation of a role-based information access level.

Demands for an Electronic Health Care System Data should be stored centrally and consistently for all healthcare actors that access it. There should also always be solutions for non-tech-savvy patients as well as a fallback mechanism. Functionality such as automatic pre-diagnoses was mentioned to assist professionals. In addition, patient burden should be kept low.

4 Discussion

Privacy Believes versus Practices Participants use insecure mediums and adopt privacy-critical practices to share data while stating that they are aware of security and privacy issues of their actions. They also state that the actions sometimes go against official process recommendations. The justification is the need to solve a medical problem and to treat the patient more efficiently, which would not be possible or at least not as quick with the recommended or privacy-preserving processes.

Requirements for a Privacy-Conscious and Efficient Treatment Patients should give their informed consent before their data is entered in any system. Ideally, this includes an extended explanation of the consequences of consenting. The patient should also have access to their data and control but at the same time, the patient's burden should be kept to a minimum. This also goes for the time-limited health experts. Any system they use to manage or share patient data should be fast, easy to access, and be integrated seamlessly into their work day while also being secure and privacy-preserving.
We see that these demands can hardly be reconciled in a system. It is not trivial to educate people about the privacy implications of digital systems, and it would also require health professionals to be able to inform patients about these issues. This goes against the wish for a quick and easy handling of these problems that does not stand in the way of an efficient treatment.

[1] https://mural.co/