SoK: Analysis of User-Centered Studies Focusing on Healthcare Privacy & Security

Faiza Tazi[1], Archana Nandakumar[2], Josiah Dykstra[3], Prashanth Rajivan[2], Sanchari Das[1]
University of Denver[1], University of Washington[2], Designer Security[3]

Abstract

Sensitive information is intrinsically tied to interactions in healthcare, and its protection is of paramount importance for achieving high-quality patient outcomes. Research in healthcare privacy and security is predominantly focused on understanding the factors that increase the susceptibility of users to privacy and security breaches. To understand further, we systematically review 26 research papers in this domain to explore the existing user studies in healthcare privacy and security. Following the review, we conducted a card-sorting exercise, allowing us to identify 12 themes integral to this subject such as "Data Sharing," "Risk Awareness," and "Privacy." Further to the identification of these themes, we performed an in-depth analysis of the 26 research papers report on the insights into the discourse within the research community about healthcare privacy and security, particularly from the user perspective.

1 Motivation

Security and privacy integration in the healthcare domain is essential to protect patients' data [12], considering medical records include sensitive health and personal information. The healthcare industry is often a prime target for cybercriminals considering that these data sets could contain a plethora of sensitive information such as social security numbers, birth dates, employment information, emergency contacts, and insurance and billing data; these data are also notoriously difficult to monitor or safeguard after a breach [23]. Furthermore, healthcare data are lucrative on the black market. Sahi et al. noted that sensitive medical data are sold for an average of $40-50 per record [34]. In light of this and to understand what is studied on the healthcare data privacy and security from the user side in research literature, we conducted a systematic literature review.

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

2 Method

We conducted a systematic literature review including a corpus of 129 papers published up to December 10, 2021 of user studies with a focus on privacy and security of healthcare patients' data. Papers were excluded if they were presented as a work-in-progress (posters, extended abstracts, less than 4 pages long, etc.). We collected papers from seven digital databases: ACM Digital Library (DL), Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. After the initial search to obtain the keywords, we collected the papers using keywords like *Healthcare Data Security, Healthcare Data Breach, Healthcare Data Theft, Medical Data Theft, Medical Data Security, Medical Data Breach, Patient Data Security, Patient Data Theft, and Patient Data Breach* through the Publish or Perish [1] software for retrieving articles from Google Scholar. After removing any duplicate articles we were left with 129 papers. We adapted the study design from prior systematic reviews [7–9, 11, 26, 30, 36, 38, 39].

After analyzing the full text of the 129 papers, we excluded 49 papers from the set because the works though mentioned healthcare and the concerns of the data from the privacy and security lenses as a motivational factor were not directly focused on privacy and security of healthcare data. From the remaining $n = 80$ papers, we consolidated the papers which consistently addressed healthcare data privacy and security throughout various stakeholders' perspective. We were left with 26 papers on which we conducted a card-sorting exercise involving all authors.

[1] https://harzing.com/resources/publish-or-perish

3 Results

Risk perception: It is challenging to circumscribe the perception of risk as risks do not have the same meaning for everyone. That is why user studies focusing on risk perception are critical, especially for the subject. Papers were categorized in the risk perception label when part of the study or its entirety explored participants' attitudes, and opinions on risks related to healthcare data. Risk perception was the most frequent label in our corpus where 61.54% of the papers were within this category.

Data sharing: 14 papers aimed to understand the perspective of participants on data sharing practices that would be acceptable to patients and beneficial to research communities. Results from these papers indicating that patients support data sharing if it benefits the public, or if the data is shared for personal health purposes. Nonetheless, people still have reservations about the privacy of sensitive data, data breaches, and medical bias.

Electronic Health Records (EHR): We found eight papers in our corpus pertaining to user interactions with EHR. These papers confirm through their results that participants have concerns over privacy and security, and are prudent about using EHR technologies. It was also determined that providers' reassurance positively impact patients' continuous and systematic usage of patient portal software in general and lowers their security concerns.

Risk Awareness: Despite the abundant potentialities for cyber risk in the healthcare sector [2], there is a startling level of naiveté among some healthcare providers. The results from the 8 papers relevant to risk awareness, show that the knowledge levels of providers regarding patient privacy, confidentiality and data sharing practices is average or lower.

Technology Adoption: Technology adoption in the healthcare domain is crucial to its development. To this regard, eight papers in our corpus examined factors and inspected participants' requirements to improve user acceptance and adoption of some healthcare technologies. The results reported by these papers reveal that the security and privacy aspects bolster the acceptance and adoption of healthcare technologies.

Regulatory Compliance: Seven papers studied the ethical and legal aspects of healthcare data management. These papers mainly assess the HIPAA compliance of participants, as well as the cybersecurity conditions and behavior of healthcare practitioners and organizations. According to the CDC, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge" [16]. Notably all the studies here determined that there needs to be more policies and reinforcement of behavior which can impede security.

Individual Differences: Comparisons can be based on experience level, hospital size, marriage status, country of origin, health status, or gender. We found seven papers from our corpus who did this type of analysis. In particular, Wilkowska and Ziefle show that females and healthy adults demand the highest security and privacy standards compared to males and the ailing elderly [41]. A different study, investigated the extent to which security policies impact health information interoperability at different levels within the same hospitals [37].

Secure Communications: In the case of healthcare, secure communications is not just a matter of security and privacy, but it can also be a medical concern. We categorized five papers within this label. Most of these papers have results that show that patients still do not fully trust the existing communications technologies, except for Elger's study [14] where 85% of the participants had no privacy concerns regarding using a secure SMS system for private medical communications.

Mobile Applications: Three papers were related to mobile applications. These papers evaluate users' perceptions of mobile health apps regarding privacy, security, and quality of care. The results of these papers were somewhat different, where Schnall et al. [35] found that the majority of their participants were concerned over privacy of their sensitive healthcare data and people having access to their healthcare data. On the other hand, both Giguere et al. [18] and Richardson and Ancker's [33] studies found that the majority of participants are unconcerned about privacy when using such apps.

Social Influence: Three papers in our corpus were categorized as social influence. These papers proved that participants were influenceable. Namely, Moqbel et al. [29] demonstrated that health professionals' reassurance and encouragement positively impact patients' continuous and systematic usage of patient portal software; not only that but participants were also influenced to lower their security concerns through the same encouragement.

Privacy: Most of the papers in our corpus touch upon privacy, but three of these papers were directed exclusively towards the privacy of healthcare data. Accordingly, in their study Elger [14] assesses the knowledge and perceptions of physicians on healthcare data violations of privacy; results show that 11% of the participants recognized all the confidentiality violations in the test cases they were presented with.

Contact Tracing: Only two papers were categorized as contact tracing. With the emergence of digital contact tracing applications, users have expressed privacy and security concerns [5]. These concerns stem from apprehension of data breaches or having their data collected by government entities [19]. However, this did not deter participants from approving COVID-19 contact tracing apps.

We have provided the details of the papers and the themes including the snapshot in the card sorting exercise in the Appendix A.

References

[1] Abimbola Adanijo, Caoimhe McWilliams, Til Wykes, Sagar Jilka, et al. Investigating mental health service user opinions on clinical data sharing: qualitative focus group study. *JMIR mental health*, 8(9):e30596, 2021.

[2] Mohiuddin Ahmed and Abu SSM Barkat Ullah. False data injection attacks in healthcare. In *Australasian Data Mining Conference*, pages 192–202, Singapore, 2017. Springer, Springer Singapore.

[3] Ala Sarah Alaqra, Bridget Kane, and Simone Fischer-Hübner. Machine learning–based analysis of encrypted medical data in the cloud: Qualitative study of expert stakeholders' perspectives. *JMIR human factors*, 8(3):e21810, 2021.

[4] Aubrey Baker, Laurian Vega, Tom DeHart, and Steve Harrison. Healthcare and security: Understanding and evaluating the risks. In *International Conference on Ergonomics and Health Aspects of Work with Computers*, pages 99–108. Springer, 2011.

[5] Eugene Y Chan and Najam U Saqib. Privacy concerns can explain unwillingness to download and use contact tracing apps when covid-19 concerns are high. *Computers in Human Behavior*, 119:106718, 2021.

[6] Lynne Coventry, Dawn Branley-Bell, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Kalliopi Anastasopoulou. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *International Conference on Human-Computer Interaction*, pages 105–122. Springer, 2020.

[7] Sanchari Das et al. Sok: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review. In *Proceedings of the workshop on usable security and privacy (USEC)*, 2022.

[8] Sanchari Das, Andrew Kim, Zachary Tingle, and Christena Nippert-Eng. All about phishing exploring user research through a systematic literature review. In *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[9] Sanchari Das, Bingxing Wang, Zachary Tingle, and L Jean Camp. Evaluating user perception of multi-factor authentication: A systematic review. In *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[10] Patricia A Deverka, Dierdre Gilmore, Jennifer Richmond, Zachary Smith, Rikki Mangrum, Barbara A Koenig, Robert Cook-Deegan, Angela G Villanueva, Mary A Majumder, and Amy L McGuire. Hopeful and concerned: public input on building a trustworthy medical information commons. *Journal of Law, Medicine & Ethics*, 47(1):70–87, 2019.

[11] Reyhan Düzgün, Naheem Noah, Peter Mayer, Sanchari Das, and Melanie Volkamer. Sok: A systematic literature review of knowledge-based authentication on augmented reality head-mounted displays. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–12, 2022.

[12] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, 19(2):326, 2019.

[13] Josiah Dykstra, Rohan Mathur, and Alicia Spoor. Cybersecurity in Medical Private Practice: Results of a Survey in Audiology. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pages 169–176, 2020.

[14] Bernice S Elger. Violations of medical confidentiality: opinions of primary care physicians. *British Journal of General Practice*, 59(567):e344–e352, 2009.

[15] Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow. Improving individual acceptance of health clouds through confidentiality assurance. *Applied Clinical Informatics*, 7(04):983–993, 2016.

[16] Center for Disease Control and Prevention. Excel snafus causes the loss of 16K UK COVID cases. https://cloudsek.com/threatintel/excel-snafus-causes-the-loss-of-16k-uk-covid-cases-un-shipping-agency-forced-offline-after-cyberattack-and-more/, Oct 2020.

[17] Fiona Fylan and Beth Fylan. Co-creating social licence for sharing health and care data. *International Journal of Medical Informatics*, 149:104439, 2021.

[18] Rebecca Giguere, William Brown III, Ivan C Balán, Curtis Dolezal, Titcha Ho, Alan Sheinfil, Mobolaji Ibitoye, Javier R Lama, Ian McGowan, Ross D Cranston, et al. Are participants concerned about privacy and security when using short message service to report product adherence in a rectal microbicide trial? *Journal of the American Medical Informatics Association*, 25(4):393–400, 2018.

[19] Farkhondeh Hassandoust, Saeed Akhlaghpour, and Allen C Johnston. Individuals' privacy concerns and

adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, 28(3):463–471, 2021.

[20] Mohammad S Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. Why employees (still) click on phishing links: investigation in hospitals. *Journal of Medical Internet Research*, 22(1):e16775, 2020.

[21] Reema Karasneh, Abdel-Hameed Al-Mistarehi, Sayer Al-Azzam, Sawsan Abuhammad, Suhaib M Muflih, Sahar Hawamdeh, and Karem H Alzoubi. Physicians' knowledge, perceptions, and attitudes related to patient confidentiality and data sharing. *International Journal of General Medicine*, 14:721, 2021.

[22] Anastasia Kozyreva, Philipp Lorenz-Spreen, Stephan Lewandowsky, Paul M Garrett, Stefan M Herzog, Thorsten Pachur, and Ralph Hertwig. Psychological factors shaping public responses to covid-19 digital contact tracing technologies in germany. *Scientific Reports*, 11(1):1–19, 2021.

[23] Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and D Kyle Monticone. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1):1–10, 2017.

[24] Juhee Kwon and M Eric Johnson. Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, 20(1):44–51, 2013.

[25] EunWon Lee and GyeongAe Seomun. Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *International Journal of Environmental Research and Public Health*, 18(4):2084, 2021.

[26] Ritajit Majumdar and Sanchari Das. Sok: An evaluation of quantum authentication through systematic literature review. In *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, 2021.

[27] Desla Mancilla and Jackie Moczygemba. Exploring medical identity theft. *Perspectives in health information management/AHIMA, American Health Information Management Association*, 6(Fall), 2009.

[28] Isma Masood, Yongli Wang, Ali Daud, Naif Radi Aljohani, and Hassan Dawood. Privacy management of patient physiological parameters. *Telematics and Informatics*, 35(4):677–701, 2018.

[29] Murad Moqbel, Barbara Hewitt, Fiona Fui-Hoon Nah, and Rosann M McLean. Sustaining patient portal continuous use intention and enhancing deep structure usage: Cognitive dissonance effects of health professional encouragement and security concerns. *Information Systems Frontiers*, pages 1–14, 2021.

[30] Naheem Noah and Sanchari Das. Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. *Computer Animation and Virtual Worlds*, page e2020, 2021.

[31] Emily C O'Brien, Ana Maria Rodriguez, Hye-Chung Kum, Laura E Schanberg, Marcy Fitz-Randolph, Sean M O'Brien, and Soko Setoguchi. Patient perspectives on the linkage of health data for research: insights from an online patient community questionnaire. *International Journal of Medical Informatics*, 127:9–17, 2019.

[32] Kalamullah Ramli et al. Hipaa-based analysis on the awareness level of medical personnel in indonesia to secure electronic protected health information (ephi). In *2021 IEEE International Conference on Health, Instrumentation & Measurement, and Natural Sciences (InHeNce)*, pages 1–6. IEEE, 2021.

[33] Joshua E Richardson and Jessica S Ancker. Public Perspectives of Mobile Phones' Effects on Healthcare Quality and Medical Data Security and Privacy: A 2-Year Nationwide Survey. In *AMIA Annual Symposium Proceedings*, volume 2015, page 1076. American Medical Informatics Association, 2015.

[34] Muneeb Ahmed Sahi, Haider Abbas, Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A Orgun, Waseem Iqbal, Imran Rashid, and Asif Yaseen. Privacy preservation in e-healthcare environments: State of the art and future directions. *IEEE Access*, 6:464–478, 2017.

[35] Rebecca Schnall, Tracy Higgins, William Brown, Alex Carballo-Dieguez, and Suzanne Bakken. Trust, perceived risk, perceived ease of use and perceived usefulness as factors related to mhealth technology use. *Studies in Health Technology and Informatics*, 216:467, 2015.

[36] Sunny Shrestha, Esa Irby, Raghav Thapa, and Sanchari Das. Sok: a systematic literature review of bluetooth security threats and mitigation measures. In *International Symposium on Emerging Information Security and Applications*, pages 108–127. Springer, 2022.

[37] Utkarsh Shrivastava, Jiahe Song, Bernard T Han, and Doug Dietzman. Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? a cross-country investigation. *International Journal of Medical Informatics*, page 104401, 2021.

[38] Elizabeth Stowell, Mercedes C Lyson, Herman Saksono, Reneé C Wurth, Holly Jimison, Misha Pavel, and Andrea G Parker. Designing and evaluating mhealth interventions for vulnerable populations: A systematic review. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2018.

[39] Faiza Tazi, Josiah Dykstra, Prashanth Rajivan, and Sanchari Das. Sok: Evaluating privacy and security vulnerabilities of patients' data in healthcare. In *International Workshop on Socio-Technical Aspects in Security*, pages 153–181. Springer, 2022.

[40] Aksel Tjora, Trung Tran, Arild Faxvaag, et al. Privacy vs usability: a qualitative exploration of patients' experiences with secure internet communication with their general practitioner. *Journal of Medical Internet Research*, 7(2):e368, 2005.

[41] Wiktoria Wilkowska and Martina Ziefle. Privacy and data security in e-health: Requirements from the user's perspective. *Health Informatics Journal*, 18(3):191–201, 2012.

[42] Rong Yin, Katherine Law, David Neyens, et al. Examining how internet users trust and access electronic health record patient portals: Survey study. *JMIR Human Factors*, 8(3):e28501, 2021.

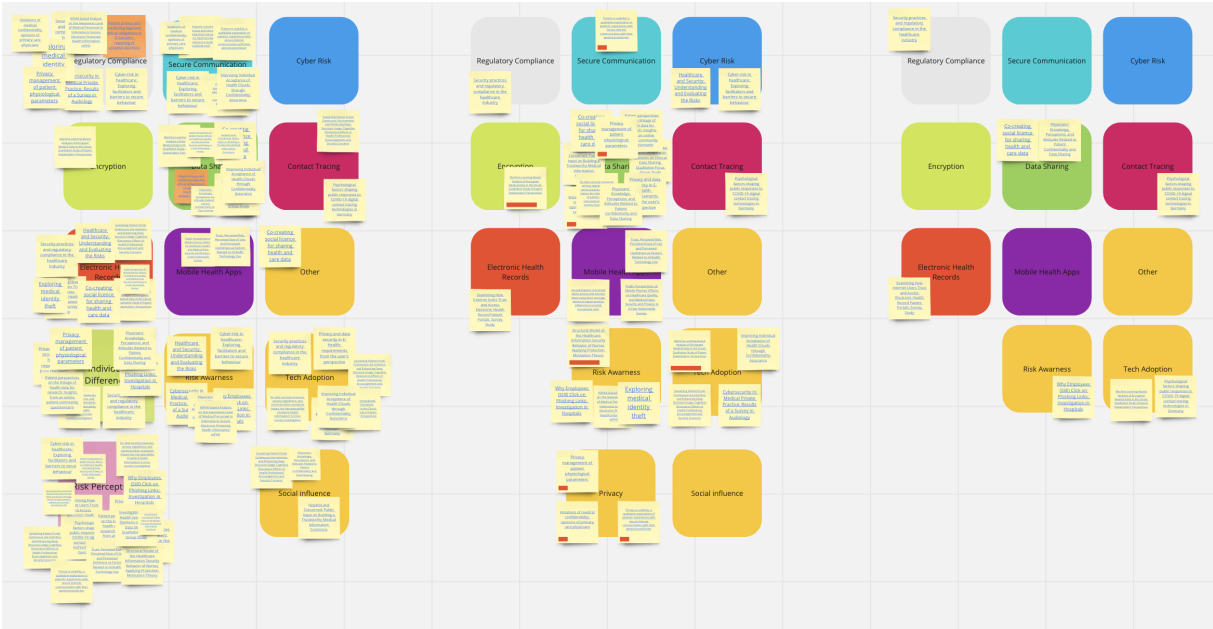

Figure 1: A snapshot of the card-sorting exercise by the researchers of the paper used to analyze the paper repository.

A Overview of Security-Focused User Studies

Study	Goal	Methods	Principal Findings	Labels
[20]	Understand reasons why hospital employees click on phishing emails	Quantitative: partial least squared structural equation modeling	Workload has a significant negative effect on secure behavior	
[18]	Assess participants' attitudes towards privacy and security while using system developed for a medical study	Mixed Methods: descriptive statistics + analysis of variance for quantitative data, thematic analysis for qualitative data	The majority of participants are unconcerned about privacy and confidentiality when using SMS despite the fact that some participants expressed their concern about possible data leaks	
[13]	Assess HIPAA compliance, cybersecurity conditions and behavior of healthcare practitioners in private practices	Quantitative: descriptive statistics	9.9% of the participants confirm they experienced at least one data breach in 2019 24.4% participants claim they have cyber insurance	
[24]	Assess security practices of healthcare organizations	Quantitative: Ward's cluster analysis using minimum variance	Participating hospitals were clustered into three clusters:leaders, followers, and laggers Hospitals prioritize technical security solutions and data privacy over security management processes and performing regular audits	
[25]	Assess nurses' health information security (HIS) practices	Quantitative: exploratory + confirmatory factor analysis	The participant nurses' HIS intentions are affected by the amount of HIS losses they are able to handle"coping appraisal" ($estimate = -1.477$, $p < 0.01$) HIS intentions have a considerable impact on coping appraisal ($estimate = 0.515$, $p < 0.001$)	
			Continued on next page	

Table 1 – continued from previous page

Study	Goal	Methods	Principal Findings	Labels
[28]	Evaluate the extent to which access to patients' physiological parameters (PPP) in hospitals can infringe on the patients' privacy	Quantitative: bivariate analysis	Patients need to have control over their own PPPs Specialists are the more trusted than family doctors, nurses, and medical assistants	
[21]	Evaluate physicians' perceptions and understanding of confidentiality and medical data sharing	Quantitative: Pearson's correlation + Multiple regression	Physicians' mean score for knowledge regarding patient confidentiality and data sharing is 7.34 out of 14 and is positively correlated with their attitudes towards the subject matter which leads to privacy breaches	
[41]	Evaluate users' attitudes towards privacy and security of medical technology	Mixed Methods: One-way ANOVA + F-Tests + Spearman's rank correlations for quantitative data and thematic analysis for qualitative data	Participants with better health value privacy and security of medical technologies and control over data access more than participant with poor health	
[33]	Evaluate the perceptions of users of mobile health applications regarding privacy, security and quality of care	Quantitative: multivariable logistic models + bivariate analysis	In 2014 participants were more likely to think that mhealth improves the quality of healthcare, however they were just as concerned about privacy in 2013 (74%) as in 2014 (75%)	
[3]	Evaluate the perceptions of experts on using ML based privacy enhancing technologies (PETs) that enable automated analysis of encrypted healthcare data stored in the cloud	Qualitative: thematic analysis	Technical experts admonish prudence in trusting ML based PETs Medical experts call for patient safety assurances regarding these tools	
[37]	Investigate the extent at which security policies impact health information interoperability at different levels within the same hospitals	Quantitative: logistic models	Hospitals with access control implemented in workstations are 44% less likely to encounter technical interoperability (TI) issues. Hospitals using one EMR are 53% less like to encounter TI issues compared with hospitals using numerous EMR systems	
[29]	Assess the influence of healthcare providers' encouragement and patient security concerns in patient portal software continued usage	Quantitative: partial least squares structural equation modeling	Providers' reassurance and encouragement has a positive impact on patients' continuous use and systematic usage of patient portal software and lowers their security concerns	
[42]	Evaluate users' perceptions and trust factors in patient portal software	Quantitative: logistic models	Participants who value their portals for managing their healthcare are more likely to trust their portals.	
[31]	Evaluate Patients' perceptions of the risks and advantages of linking existing research data sources	Quantitative: descriptive statistics	19.7% of the participants are weary about researchers having access to their deidentified data. 90% of the participants are more assured when their unique identifiers were removed from the the dataset used for research and linkage	

Continued on next page

Table 1 – continued from previous page

Study	Goal	Methods	Principal Findings	Labels
[27]	Investigate admitting and registration protocols in hospital in order to establish best practices to curtail medical identity theft	Mixed Methods: descriptive statistics for quantitative data, thematic analysis for qualitative data	78.5% of the participants confirmed that patient identities is verified at admission or registration 91.9% of which using driver's license. If the patient shows up without proof of identity, 59.5% of the participants affirmed that they provide the service without confirming the identity of the patient	
[6]	Understand the insecure practices within healthcare	Qualitative: thematic analysis	Three main impediments for security: security viewed as a barrier to patient care and productivity, Ignorance of consequences, dearth of policies and reinforcement of secure behaviour	
[4]	Understand security and privacy practices of physicians' offices' staff	Qualitative: phenomenological approach	Several insecure behaviours were observed such as password sharing, data left in insecure areas and absence of password use	
[22]	Evaluate the public's perceptions and acceptance of contact tracing technologies	Quantitative: descriptive statistics + logistic models + chi-squared tests	In March 2020, 68% of participants declared that it was acceptable to grant the government access to citizens' medical records vs only 35% participants in November of the same year Acceptance of privacy intrusive technologies diminished over time during the pandemic.	
[10]	Investigate the public's perceptions about the important concerns in the design of medical information commons (MIC)	Qualitative: thematic analysis	There needs to be a balance between the benefits of an MIC and the safeguards it implements to keep patients' data private	
[1]	Analyse the outlook of the mental health service users on satisfactory data sharing practices	Qualitative: thematic analysis	Participants expressed concern over the security and the high risk of large datasets. Participants conveyed the necessity to preserve the privacy and confidentiality of patients while taking into consideration the people who have access to privileged data.	
[17]	Investigate the participants' perceptions on healthcare data sharing process and establishing ways to gain their trust of the process	Participants expressed concerns over being identified and security limitations of data sharing systems Participants declared that their primary care providers as well as hospital doctors and nurses should have access to their medical records	participants approve and advocate for sharing healthcare data for direct care, but not for social care. Participants expressed concerns over privacy, security limitations and potentially having providers make biased decisions based on information found in their records	
[35]	Examine the factors that contribute to patients' intention of using an HIV mobile healthcare application including security, privacy, trust, risk and usability	Qualitative: thematic analysis	Participants expressed concerns over privacy and trust of their sensitive healthcare data and the people who would have access to their healthcare data Participants worried about the perceived risks including disclosure, tracking and data leaks	

Continued on next page

Table 1 – continued from previous page

Study	Goal	Methods	Principal Findings	Labels
[15]	Investigate how promises of confidentiality contribute to the participants' willingness to accept health clouds as an infrastructure for healthcare data sharing	Quantitative: descriptive statistics + Comparison of means	The promise of privacy increases the participants acceptance of health clouds in the case of sensitive and confidential healthcare data on the other hand, no statistical significance was found in the case of non-sensitive medical data	
[32]	Assess the understanding and healthcare data security awareness levels of participants	Quantitative: descriptive statistics	Participants' knowledge is lacking: (mean=2.6 where the average should be less than 2). Hospital management has the highest security awareness levels (mean=2.0667) while physicians have the lowest (mean=2.9202)	
[14]	Assess the knowledge and perceptions of physicians on healthcare data violations of privacy and confidentiality	Quantitative: descriptive statistics + Comparison of means	Barely 11% of the participants recognized all the confidentiality violations in the test cases they were presented with	
[40]	Analyze the privacy posture of patients who use secure electronic communication systems (ECS) compared to their perception on usability of these systems	Qualitative: thematic analysis	Patients use the ECS for subjects they view as unsubstantial and avoid it for intimate or personal details	

Table 1: An Overview of the Security Focused User Studies Including Goal of each Study, Methods and Principal Findings. The symbols in the "Labels" column refer to the labels derived during the card sorting exercise: = Regulatory Compliance, = Secure Communication, = Data Sharing, = EHR , = Individual Differences, = Risk Awarness, = Tech Adoption, = Social Influence, = Risk Perception, = Mobile Healthcare, = Privacy, = Contact tracing