



# SoK: Analyzing Privacy and Security of Healthcare Data from the User Perspective

FAIZA TAZI, University of Denver, Denver, USA

ARCHANA NANDAKUMAR, University of Washington, Seattle, USA

JOSIAH DYKSTRA, Designer Security, LLC, Fort Meade, USA

PRASHANTH RAJIVAN, University of Washington, Seattle, USA

SANCHARI DAS, University of Denver, Denver, USA

Interactions in healthcare, by necessity, involve sharing sensitive information to achieve high-quality patient outcomes. Therefore, sensitive data must be carefully protected. This article explores existing privacy and security research conducted in the context of healthcare organizations. We conducted a systematic literature review of  $N = 1,553$  articles that examine the security and privacy of healthcare data and focus on 80 articles addressing human factors. Key findings show that much of the healthcare security and privacy research is focused on technology (44.11%, 712 articles), with a lack of emphasis on the human element (4.96%, 80 articles). In the subset of user studies, we find that patients and the general public express concerns about privacy and security with technologies like electronic health records (EHRs). Furthermore, our analysis shows that healthcare professionals often have low awareness of risks related to data security. Additionally, our analysis revealed that most research focuses narrowly on large hospitals, neglecting private practices and the unique challenges they face. We conclude by identifying research gaps and providing potential solutions to enable robust data security for sensitive patient data.

CCS Concepts: • **Security and privacy** → **Human and societal aspects of security and privacy**; **Usability in security and privacy**; • **Applied computing** → **Health care information systems**; • **Human-centered computing** → **Human computer interaction (HCI)**;

Additional Key Words and Phrases: Literature review, healthcare, privacy, cybersecurity, HIPAA

## ACM Reference Format:

Faiza Tazi, Archana Nandakumar, Josiah Dykstra, Prashanth Rajivan, and Sanchari Das. 2024. SoK: Analyzing Privacy and Security of Healthcare Data from the User Perspective. *ACM Trans. Comput. Healthcare* 5, 2, Article 11 (April 2024), 31 pages. <https://doi.org/10.1145/3650116>

## 1 INTRODUCTION

Security and privacy integration in the healthcare domain is essential to protect patients' data [1], considering medical records include sensitive health and personal information. A collection of such personal information has a potential for identity theft [2]. The healthcare industry is often a prime target for cybercriminals considering

This work was partially supported by a grant from Cisco.

Authors' addresses: F. Tazi and S. Das, University of Denver, 2155 E Wesley Ave, Denver, CO, 80208 USA; e-mails: Faiza.Tazi@du.edu, Sanchari.Das@du.edu; A. Nandakumar and P. Rajivan, University of Washington, 371 Loew Hall, Seattle, WA 98195, USA; e-mails: archanan@uw.edu, prajivan@uw.edu; J. Dykstra, Designer Security, LLC, Fort Meade, USA; e-mail: josiah@designersecurity.com.



This work is licensed under a Creative Commons Attribution International 4.0 License.

© 2024 Copyright held by the owner/author(s).

ACM 2637-8051/2024/04-ART11

<https://doi.org/10.1145/3650116>

that these datasets 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 [3]. 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 [4]. At the same time, Coventry and Branley revealed that the value for a complete set of medical credentials could fetch over \$1,000 [5]. The magnitude of financial profit from these transactions creates a strong interest from cybercriminals causing healthcare organizations to be more inviting targets for attackers [2]. According to the National Audit Office, the 2017 WannaCry ransomware attack that impacted the **National Health Service (NHS)** in the United Kingdom is considered the most significant affecting a healthcare organization in recorded history. The National Audit Office identified that significantly more devastation would likely have occurred if the WannaCry ransomware had not been disrupted by coincidence when a cybersecurity analyst discovered a “phone home” mechanism by accident.

The exchange of patient and care data between healthcare professionals is integral to effective patient outcomes. In this work, healthcare professionals (also called providers) are people who give medical, health, dental, pharmaceutical, and any other healthcare services. In the United States, these individuals are licensed, registered, or certified to provide healthcare services under Federal or State laws or regulations. Current research in the healthcare privacy and security field strives to understand factors that make users (both patients and healthcare professionals) more vulnerable to security and privacy breaches. As with many other sectors, data breaches in healthcare occur for various reasons: from lack of employee awareness about data security to technological shortcomings to the dearth of robust technological implementations [6]. For example, in one recent assessment, employees in US health institutions clicked on at least 1 in 7 simulated phishing links [7].

Designing a secure system of data sharing that keeps privacy intact while also being usable by the humans interacting with the system is a complex “systems” problem. Studies that examined user adoption of security and privacy technology solutions confirm users’ preference for usability and unwillingness to sacrifice privacy [8]. While the technology and design frameworks used for creating these systems are crucial, it’s equally important to understand the human aspect of healthcare privacy and security. Given the growing need to protect critical health information [9], the field lacks a comprehensive synthesis and analysis of the body of healthcare privacy and security research, especially from a human factors perspective [10, 11]. Throughout this work, we refer to all individuals with access and responsibility for protecting healthcare data as *users*, including patients and healthcare workers with direct or indirect contact with patients.

In light of this, we conducted a systematic literature review to provide a holistic overview of the research undertaken in this area which has been proven helpful in other domains [12]. We collected 5,520 research articles related to data security and privacy preservation in healthcare organizations. After that, we did a thematic analysis on a selected set of  $N = 1,553$  articles. From the  $N = 1,553$  articles, we further analyzed 80 articles that focused on the user perspective. Finally, we present an in-depth analysis of  $n = 26$  articles selected from the user study articles that focused on the security and privacy of healthcare data. Our analysis identified 12 overarching themes namely: “Risk Perception,” “Data Sharing,” “EHR Interactions,” “Risk Awareness,” “Technology Adoption,” “Regulatory Compliance,” “Individual Differences,” “Secure Communications,” “Mobile Applications Interactions,” “Social Influence,” “Privacy,” and “Contact Tracing.” Our collected data corpus consisted of peer-reviewed and published full articles. We found that most of the security research done in healthcare tended to be technology-focused, with a severe lack of focus on understanding and improving the human factor. Furthermore, even among the works focused on technologies, we observed a need for more work with applications to private practice healthcare organizations. Within the user studies, we find that both patients and the general public voice their apprehensions regarding the privacy and security of their healthcare data. Nevertheless, they continue to support the sharing of this data for the benefit of research and direct medical treatment. Furthermore, our analysis indicates that healthcare professionals lack sufficient knowledge about the potential dangers associated with data security. However, providing training to healthcare practitioners on

fundamental principles of healthcare privacy and security can positively impact risk awareness and technology adoption.

Our study has the following contributions to the research community:

- This study pioneers a comprehensive **Systematization of Knowledge (SoK)** centered around security and privacy in healthcare organizations. While there have been SoK articles focused on specific healthcare technologies, our work is unique in its broad and systematic approach, encapsulating a larger spectrum of concerns, especially aligning with users' perspectives as studied by prior works.
- Our SoK offers a holistic evaluation of security and privacy in healthcare, shedding light on crucial gaps in the current protective measures for patient health data. This extensive overview is instrumental for both industry professionals and researchers aiming to secure healthcare data, especially when it comes to patient data.
- Our research stands out as it is. To the best of our knowledge, this is the first SoK to not only focus on the technical aspects but also offer a comprehensive overview of research related to the privacy and security of patient data from a human-centered perspective. This dimension is crucial as it acknowledges the significance of understanding and addressing human factors in ensuring robust healthcare data protection.
- Methodologically, we have incorporated the card-sorting technique [13, 14] into our article analysis, which involves the collective insights of all authors to synthesize knowledge. The adoption of the card-sorting technique for SoK represents a novel methodological enhancement.

We conclude that:

- (1) Technological solutions are outpacing the foundational analysis of the ways the healthcare workforce is using and protecting patient data today; and
- (2) Existing research focuses on a narrow scope of medical settings, which neglects the large population of patients and healthcare workers engaged in private healthcare practices.

## 2 RELATED WORK

Several prior works considered research on various aspects of privacy and security in healthcare. One major category of systematic reviews in the field of security and privacy are works that focus on aggregating research about the usability of technological solutions such as blockchain, encryption, the internet of things, and biometrics and their applicability and effectiveness in the privacy and security of healthcare organizations. For example, Clayton et al. looked at genetic privacy in particular and aggregated survey studies that have gathered perceptions from different members of the society [15]. Alrazaq et al. looked at electronic personal health records and the factors that affect patient uptake of these records through a systematic review of research that has captured patient preferences [16]. Kruse et al. aggregated patient and healthcare professional perspectives on using patient portals for chronic disease in particular [17]. Security and privacy are often a category of interest among other interests within this category of reviews.

Another major category of systematic reviews is studies examining the overall state of cybersecurity within healthcare organizations. These focused on the overall organization, device, or mode of care. Privacy and security form a subcategory when studying the overall security of a healthcare system. There is also less focus on the user perspective, and the primary focus is the organizational perspective. Kruse et al. reviewed works that document cybersecurity attacks on hospitals [3]. The work by Jalali et al. conducted a thematic analysis of 472 articles that were discussions of cybersecurity in healthcare [18]. The work by Nifakos et al. looked at works that focused and studied the human factors of cybersecurity in healthcare organizations [19]. The authors recognized the need for improved training of healthcare professionals to improve security in healthcare organizations. While their work focused on the organizational perspective, our emphasis is on the human perspective and specifically relating to patients and healthcare professionals.

The third review category is studies that investigate some particular aspect or subdivision of healthcare and examine works of security and privacy within that umbrella. For example, some examined the security and privacy aspects of patient portals, **electronic health record (EHR)** systems, and telemedicine. These bodies of work typically focus on the security and privacy problems specific to that particular niche within healthcare. For example, Hameed et al. conducted a systematic review of security and privacy issues in the **internet of medical things (IoMT)** with a particular focus on the sophistication of machine learning techniques employed within this domain [20]. Aljedaani et al. focused on security challenges in mobile health (mHealth) applications in particular [21]. Kolasa et al. reviewed privacy and security concerns in applications used for contact tracing early in the COVID-19 pandemic [22]. Finally, Watzlaf et al. conducted a systematic review of the security and privacy challenges within the domain of telemedicine [23].

The current systematic review of literature on privacy and security in healthcare primarily focuses on technological solutions. There need to be more studies that review the user perspective (either that of the healthcare professional or the patient) in this domain. Thus, in our study, we have chosen to focus on the human aspect of privacy and security in healthcare organizations by identifying bodies of work that capture the human perspective on the subject matter. Some examples include surveys, interviews, and focus groups of patients, healthcare professionals, or other stakeholders in the healthcare organization.

### 3 METHOD

In order to better understand the landscape of the existing research on data security and privacy preservation in healthcare organizations, we conducted a systematic literature review following the “**preferred reporting items for a systematic review and meta-analysis**” (PRISMA) guideline [24]. Our systematic literature review includes a corpus of 1,553 articles published up to December 10, 2021, collected from different digital libraries. The literature review comprised six steps: (i) database search, (ii) title screening, (iii) abstract screening, (iv) full-text screening, (v) data extraction, and (vi) thematic analysis.

*Inclusion Criteria:* Articles were included if they were: (1) Published in a peer-reviewed publication, including journals and conferences; (2) Written and available in English, and (3) Focused on the security and privacy of data in healthcare organizations.

*Exclusion Criteria:* Articles were excluded if: (1) Articles were presented as a work-in-progress (posters, extended abstracts, etc.); (2) The content analysis showed that the research was not directly related to patient/consumer health-related data security and/or privacy in healthcare organizations; and (3) The collected articles were part of patents or book chapters.

Figure 1 details all the steps carried out throughout this analysis.

#### 3.1 Database and Keyword-based Search

We conducted our search by exploring seven digital technology and medical databases: **ACM Digital Library (ACMDL)**, Google Scholar, **Social Science Research Network (SSRN)**, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. Our selection process was based on an iterative evaluation. We started by defining appropriate keywords for our subject matter. This was followed by filtering the results to meet our requirements. Subsequently, we systematically analyzed the final collection of research articles. This procedure was adapted from previous literature reviews by Stowell et al. [25], Das et al. [26, 27], and other related works [28–31].

After the initial search to obtain the keywords, we collected the articles through a keyword-based search as mentioned above, using the Publish or Perish<sup>1</sup> software for retrieving articles from Google Scholar. After that, we explored individual digital libraries to collect articles relevant to this research. Boolean search strings were developed for searching databases including “AND/OR” operators as well as NOT operators across the following keyword terms: *Healthcare Data Security*, *Healthcare Data Breach*, *Healthcare Data Theft*, *Medical Data Theft*,

<sup>1</sup><https://harzing.com/resources/publish-or-perish>

Search	N= 5520	Database Search: ACM DL, Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed, Medline
	N=2032	Duplicate Removal Title Screening (Google Scholar) Quality Screening (Removal of work in progress)
	N=1553	Abstract Screening
Analysis	N = 80	Full Text Analysis: User Studies
	n = 26	Card Sorting

Fig. 1. A snapshot of the data collection, screening, and analysis methodology and the number of articles screened in each stage of the literature review.

*Medical Data Security, Medical Data Breach, Patient Data Security, Patient Data Theft, and Patient Data Breach.* Our initial database and keyword-based search resulted in a total of 5,520 articles.

### 3.2 Title Screening

We conducted title-based searches for relevant articles in several digital libraries. Google Scholar, ACM DL, and IEEE Xplore yielded substantial results, so we focused our search efforts on those databases. For the other digital libraries, we used a simplified yet broad search strategy to capture the most relevant articles.

In Google Scholar, we searched for articles with “Healthcare Data Security,” “Healthcare Data Breach,” “Healthcare Data Theft,” “Medical Data Theft,” “Medical Data Security,” “Medical Data Breach,” “Patient Data Security,” “Patient Data Theft,” or “Patient Data Breach” in the title. We excluded patents and citations, conducting multiple searches and aggregating the results to maximize coverage. This yielded 352 articles.

For ACM DL and IEEE Xplore, we used their advanced search filters to restrict our search to titles, abstracts, and keywords of journals and peer-reviewed conferences. In ACM DL, this reduced our results from over 30,000 to 2,477 relevant matches. As for IEEE Xplore, we reduced the results from over 7,000 articles to 63 articles.

In the remaining digital libraries, we used the search string: “Healthcare Data Security” OR “Healthcare Data Breach” OR “Healthcare Data Theft” OR “Medical Data Theft” OR “Medical Data Security” OR “Medical Data Breach” OR “Patient Data Security” OR “Patient Data Theft” OR “Patient Data Breach” and further constrained the parameters to limit the result set to the most relevant articles possible.

Table 1 provides the specifics of our search approach in each digital library database, including search terms used, number of articles returned, and the search filters applied.

### 3.3 Duplicate and Work-in-Progress Removal

In this phase, we proceeded to remove duplicate articles. First, we removed any duplicate articles from the different databases. We also removed any articles which were a work in progress, such as posters and extended abstracts. Finally, we screened out self-identified work-in-progress articles or reviewed the article to see if the articles were works-in-progress. Due to the varying nature of the publication of these works, we could not demarcate the articles based on their page numbers with an assumption that work-in-progress articles are short. However, we removed any articles which were shorter than four pages. After this procedure, we were left with a dataset of 2,032 articles.

Table 1. Number of Articles Found in Each Database and the Search Terms and Parameters Utilized

Database	Search Terms	# Articles	Search Parameters
ACMDL	[Title: healthcare data security] AND [Title: healthcare data breach] AND [Title: medical data breach] AND [Title: patient data theft] AND [Title: healthcare data theft] AND [Title: medical data theft] AND [Title: medical data security]	2,477	Journals + Research Article
MEDLINE	"Healthcare Data Security" + "Healthcare Data Breach" + "Healthcare Data Theft" + "Medical Data Theft" + "Medical Data Security" + "Medical Data Breach" + "Patient Data Security" + "Patient Data Theft" + "Patient Data Breach"	1,477	–
SSRN		382	Search in Title, Abstract & Keywords
Google Scholar		352	Used Publish or Perish
Pubmed	"Healthcare Data Security" OR "Healthcare Data Breach" OR "Healthcare Data Theft" OR "Medical Data Theft" OR "Medical Data Security" OR "Medical Data Breach" OR "Patient Data Security" OR "Patient Data Theft" OR "Patient Data Breach"	233	Text Availability: "Full text" + Article type: "Meta-Analysis" + "Randomized Controlled Trial" + "Review" + "Systematic Review"
ScienceDirect		184	Article type: "Review article" + "Research article"
IEEE Xplore	("Document Title":Medical Data Breach) OR ("Document Title":Patient Data Theft) OR ("Document Title": Patient Data Breach) OR ("Document Title":Healthcare Data Security) OR ("Document Title":Healthcare Data Breach) OR ("Document Title":Healthcare Data Theft) OR ("Document Title":Medical Data Theft) OR ("Document Title":Medical Data Security) OR ("Document Title":Patient Data Security)	63	Conferences + Journals

### 3.4 Abstract Screening

We assessed the 2,032 research articles in our corpus to determine their relevance to our research topic by reviewing the abstract. Three researchers trained in qualitative coding determined the relevance of the individual articles to the research by analyzing the abstract. When there were discrepancies in determining the relevance of the article, all researchers discussed these articles in more detail to resolve the issue, only articles that addressed the security or privacy of healthcare data were included. Thus, 479 articles were excluded in this phase. After this screening, there remained a total of  $N = 1,553$  articles on which we conducted two phases of thematic analysis [26].

### 3.5 Analysis

First, we conducted a thematic analysis of the abstract to classify and evaluate the articles within significant themes. After that, we conducted a detailed analysis of the user studies to understand more about the user issues as per the goal of this work.



Table 2. Inter-rater Reliability Per Category

Category	Score
Type of Study	1
Population	0.93
Study Population Setting	0.96
Study Location	0.81
Number of Participants	1

**3.5.1 Thematic Analysis:** Twenty articles were randomly selected to generate overarching themes, after which three researchers evaluated the remainder of the articles. All the researchers agreed upon the themes which included: “User Studies,” “Technical Solutions,” “Frameworks,” “SOKs and Overviews,” and “Security Reviews.” Any article that included any form of user study, even if that was not the article’s primary theme, was marked in the user study category. This was specified given the user-focused aspect of the article. After conducting the first set of analyses, we performed a more detailed set of thematic analyses to categorize the user studies; following this step, we conducted a card-sorting exercise on the most relevant user studies.

**3.5.2 User Study Analysis.** After the two phases of thematic analysis, we conducted a detailed user study analysis on 129 user studies. After a thorough analysis of the complete text, 49 articles were excluded from this set for various reasons, including needing more focus on the privacy and security of healthcare patients’ data throughout the methodology, results, and discussion. For the remaining  $N = 80$  articles, we extracted the quantitative and qualitative findings to assess what technical perspectives of the healthcare-focused research were conducted by the prior studies as well as the type of participant these studies were interested in such as medical professionals, patients, technical experts, or general public. Nine publications were selected at random for the purpose of conducting inter-rater reliability. Each article was categorized across five distinct categories. A team of three researchers meticulously evaluated these articles to ensure a comprehensive classification. Given that the inter-rater reliability rates exceeded 0.81 for all categories, as indicated in Table 2, the remaining publications were allocated to two out of the three researchers for coding purposes ensuing the same categorization.

Of these 80 articles, we consolidated a set of 26 articles centered around healthcare data privacy and security from all aspects, including the objective itself, the methods, the results, and the discussion. Furthermore, we conducted a card sorting exercise involving all authors on these 26 articles. This allowed us to understand these articles better and find connections and similarities between these articles. The first author started by identifying the 26 articles and generating the themes; afterward, two groups of two authors each organized the articles into the existing themes. The themes were not mutually exclusive, and groups were able to add themes when deemed necessary. For each of the articles in our corpus, we combine the card sorting results from all the authors.

## 4 FINDINGS AND DISCUSSIONS

In this section, we first provide the results of the thematic analysis, and after that, we provide details and evaluation of the user studies.

### 4.1 Thematic Analysis

In the following sections, we provide results for each of the five themes into which we have classified our corpus, while focusing mainly on user studies. Sections 4.1.1 to 4.1.4 present four of the themes, but the fifth theme: “User Studies” is presented in Section 4.2.

**4.1.1 Technical Solutions.** Nearly half of the collection, 712 (45.85%) out of  $N = 1,553$  articles, focused on proposing a technology-based solution for the privacy and security issues of the healthcare sector. The authors

have proposed several technological solutions to enhance the privacy and security of the data transferred and accessed in the healthcare sector; for instance, Gupta and Metha discussed the importance of transmitting medical data over an unsecured network and proposed a chaos-based encryption scheme to secure medical images. In their algorithm, they use a combined key sequence of logistic map and Duffing map by shuffling the adjacent pixels of the medical data where the encryption and decryption keys are combined using the XOR function to obtain a single key sequence. Their proposed scheme was proven functional against access-control-based attacks [32]. Another critical focus on the technological solutions found in our collected sample was on the blockchain. For instance, Brunese et al. proposed a blockchain-based technology aimed at protecting information exchanges in hospital networks, with particular regard to magnetic resonance images by implementing formal equivalence checking to validate the network of the transiting data [33]. On a different note, Tian et al. looked into clinical prognosis prediction models based on EHR data. They developed a web service based on multi-center clinical data called POPCORN. The **PrognOsis Prediction based on multi-center clinical data CollabORatioN (POPCORN)** focused on the standardization of clinical data expression, the preservation of patient privacy during model training using a multivariable meta-analysis, and a Bayesian framework [34].

**4.1.2 Healthcare Frameworks.** Of the 1,553 articles collected, 390 (25.11%) articles studied or introduced new healthcare data management frameworks. We considered an article under the theme of *healthcare frameworks* if the main subject of its study is a security, privacy, or design framework, or if it introduced or analyzed a legal or ethical framework. These articles mainly describe methods to design a secure and private technology for healthcare data usage. One such article, “A Security Framework for Mobile Health Applications,” introduced a security framework for mobile healthcare applications, taking usability and security into consideration [35]. Ibrahim et al. introduced a framework for securely sharing EHRs over the cloud between different healthcare professionals. This framework ensures the confidentiality, integrity, authenticity, availability, and auditability of EHRs [36]. Similarly, Zalloum and Alamlah proposed a privacy-preserving framework for medical data sharing in their article; they also designed a digital information system that restricts access to medical information unless the patient approves the access [37]. Jia et al. followed a different approach with their privacy-preserving medication adherence framework. In their proposed framework patients are given control over how their information is transmitted and shared [38].

**4.1.3 Systematic Literature Reviews and Overviews.** Of the 1,553 articles analyzed, 228 (14.68%) were systematic literature reviews or overviews. These studies gave an overview of the current standards and practices followed in the healthcare sectors or consolidated the prior work on this sector while mentioning the importance of the focus on healthcare privacy and security. However, these studies should have focused on or explored the user perspective. For example, Walker et al. implemented a mixed-method systematic review by analyzing about 300,000 articles and found evidence of high heterogeneity across crude data indicating that the effectiveness of security measures varies significantly in healthcare but concluded without a solution for insider attack [39]. Similarly, Paksuniemi et al. give an overview of the wireless technologies devices and reveal the importance of implementing security measures in these technologies to enable secure patient monitoring [40]. Moreover, Wang provides an overview of the security threats imposed by smart devices which monitor patients through internet-connected technologies. Wang details two primary security-related issues for internet-based telemedicine systems that need to be addressed: (1) medical data protection needs; and (2) system design issues [41].

**4.1.4 Security Evaluations and Data Breaches.** We classified 143 articles as a security evaluation or data breach theme if they provided an insight or assessment of the security state of the healthcare sector and the technologies used in this area. Articles were also included in this theme if they provided the state, history, or technical details on security violations in the healthcare sector. For example, one such article documents cyber security threats and methodologies in the healthcare domain, pointing out how to analyze and manage them [42]. Furthermore, Spanakis et al. introduce a multi-layer attack model providing a new attack and threat identification and analysis



method. In a similar vein, Lopatina et al. analyze possible risks associated with the IoMT devices and systems and evaluate the threat impact and the cyber threat consequences on patients and the medical organizations using them as a whole [43]. Furthermore, Romanovs et al. analyze the cybersecurity healthcare situation in the world and examine the principal integration problems in telemedicine that prevent healthcare professionals from affording remote medical help safely and efficiently [44].

## 4.2 Analysis of User Studies

In addition to our analysis of the technical solutions discussed in the collection, we performed a detailed analysis of the user studies ( $N = 80$ ). Our goal was to understand and assess the studies that evaluated human factors of data security and privacy in healthcare. Therefore, we thoroughly analyzed the user studies and specific aspects of the study, such as the type of study conducted, study populations, duration, and medical settings.

**4.2.1 Study Method.** Of the 80 user studies in our corpus, 65% (52) were quantitative studies. From the quantitative perspective, one was a cross-sectional survey [45], another was a cross-sectional survey with repeated measures [46], and one used Q-methodology [47]. Furthermore, one study was a quantitative descriptive study [48], and one was a simulation-based study for a quantitative sample [49]. The remaining 48 articles were various forms of surveys, including online surveys, phone surveys, postal surveys, or field surveys [50–96]. On the other hand, 21.15% (11) were mixed-methods including seven articles that used multi-stage studies [97–101]. Furthermore, [102–106] used structured surveys with both open-ended and closed-ended questions. The responses were then quantitatively and qualitatively analyzed, and finally [8] did a user study on a web-based electronic healthcare records system launched by the Veterans Administration called MyHealthVet. Of other studies, one was a field study [107], one was a comparative analysis [108], six were qualitative focus group-based studies [109–114], and nine were interview-based studies [115–123].

Among the 80 user studies, only two assessed a proposed technological intervention. For example, Abd-alrazaq and colleagues measured the efficiency and convenience of a mobile app for managing diabetes evaluation [120]. In this work, participants noted that one advantage of it was compliance with hospital regulations for patient data security. On the other hand, Haggstrom et al. assessed the usability of the MyHealthVet program, where participants expressed concerns about the privacy of reviewing medical data at home [8].

One qualitative study conducted a comparison analysis on smart contract blockchains for healthcare applications [108]. Yu et al. recruited three students with no former experience in blockchain technologies to construct and test three pre-selected blockchain platforms and examined the practical aspects of the experiments. Through their study, Yu et al. established that the choice of an appropriate platform is contingent upon the specific needs of the application.

**4.2.2 Study Duration.** For the majority of the quantitative studies, the time taken for the completion of the study primarily occurred in a single session (Table 3) [45–59, 61, 62, 64–90, 92–96, 106], with the exception of three articles, where multiple surveys were deployed. In the first one, a survey of public perception of mobile phones' effect on healthcare was repeated in 2013 and 2014 [91]. The findings of this study revealed a growing inclination among participants to believe that such utilization of mHealth will lead to improvements in the overall quality of healthcare. While there was no observed year-over-year growth in participants' privacy and security worries, it is evident that participants still have significant apprehensions in this regard. The second article also conducted two surveys with a one-year gap, the first of which consisted of a baseline survey in 2012 before an educational outreach intervention and a follow-up survey in 2013 to evaluate communication between healthcare professionals [60]. This study found that the implementation of physician champion educational outreach initiatives resulted in a notable rise in the utilization of secure provider-to-provider EHR system messaging services. Finally, the last study implemented a survey on two separate occasions, initially in December 2013 and subsequently in September 2015 [63]. This was done following a modification in the EHRs

Table 3. Percentage and Number of Studies in Settings with Various Population Densities and Details about the User Study Durations

	Qual Studies (n = 17)	Quant Studies (n = 52)	Mixed-Methods (n = 11)
<b>Population</b>			
Urban	11.76% (2)	7.69% (4)	9.09% (1)
Rural	17.65% (3)	0% (0)	18.18% (2)
Mixed	5.88% (1)	7.69% (4)	9.09% (1)
Other	0% (0)	0% (0)	0% (0)
Not reported	64.71% (11)	84.62% (44)	63.64% (7)
<b>Study Population Setting</b>			
Healthcare Providers	23.53% (4)	26.92% (14)	18.18% (2)
Healthcare Students	5.88% (1)	5.77% (3)	0% (0)
Patients	17.65% (3)	13.46% (7)	27.27% (3)
Technical experts	5.88% (1)	7.69% (4)	9.09% (1)
Mixed	29.41% (5)	19.24% (10)	18.18% (2)
General Population	17.65% (3)	26.92% (14)	27.27% (3)
<b>Study Location</b>			
USA	47.06% (8)	25% (13)	45.45% (5)
Europe	29.41% (5)	25% (13)	27.27% (3)
Transcontinental	0% (0)	1.92% (1)	9.09% (1)
Asia	0% (0)	21.15% (11)	0% (0)
Middle East	5.88% (1)	9.61% (5)	9.09% (1)
Africa	5.88% (1)	1.92% (1)	0% (0)
Turkey	0% (0)	1.92% (1)	0% (0)
Oceania	0% (0)	5.78% (3)	9.09% (1)
South America	0% (0)	1.92% (1)	0% (0)
Not reported	11.76% (2)	5.78% (3)	0% (0)

system utilized by the hospital where the study was conducted. The objective of the study was to assess the level of influence exerted by the three primary categories of clinical staff (physicians, paraprofessionals, and administrative personnel) on the intention to adopt an EHRs system, as well as its underlying factors. All of the hypotheses pertaining to the personnel are validated in this study. Specifically, anxiety, self-efficacy, and trust are found to have an influence on ease of use. Additionally, ease of use, misfit, self-efficacy, and data security are found to impact the intentions to use the EHR. However, the perception of ease of use of EHR among staff and assistants does not have a significant impact on their intentions to use EHRs. Such longitudinal studies are critical to understanding how user perspectives about security and privacy can change (or do not change) over time.

As for qualitative studies, all but one of the studies were conducted in a single session. The sole exception was an evaluation of a diabetes management app for 6 to 12 weeks where participants' interactions with the app were tracked and recorded [120]. After this phase of the study, participants were then asked to take an interview to discuss their individual experiences with the app.

Similarly, the mixed methods studies consisted of few single-session studies [8, 102–105] and few comprehensive studies. One such extended study was particularly elaborate and included a postal survey to understand participants' perceptions towards the electronic transfer of medical prescriptions [66]. This study revealed that the electronic transmission of prescription-related data is expected to be well-received by all participants. However, authors note that it is crucial to address apprehensions regarding patient confidentiality. In addition, participants accessed their EHRs for the first time and answered questions about their experience using the

system. Finally, focus groups were conducted to assess participants' attitudes towards various aspects of the EHR system [98]. Pyper et al. found that most participants were satisfied with the computer technology employed, furthermore, the majority of participants expressed that they found the act of reviewing their medical records to be beneficial and were able to comprehend the majority of the information included within, however, participants expressed apprehension on the aspects of security and confidentiality, particularly with regards to the possible exploitation of their records. Similarly, another comprehensive study used focus groups, a survey, case study cards, and co-creation workshops to measure the participants' attitudes toward data sharing and develop standards for acceptable data sharing [97]. The participants of the focus group expressed their endorsement for the sharing of health and care data specifically to facilitate direct care, however, they were also apprehensive about the reliability and accuracy of their records, as well as potential social disapproval linked to certain diagnoses, particularly those related to mental health. Furthermore, participants expressed concerns regarding the identification of individuals, the constraints imposed by security measures, and the possibility of care allocation being influenced by information contained in their records, including their lifestyle preferences [97]. In addition, one study used surveys and semi-structured interviews to evaluate patients' concerns about data sharing in the context of HIV patients [101]. Maiorana et al. argue that both patients and healthcare professionals demonstrate a willingness to embrace the electronic exchange of HIV patient data as a means to enhance the quality of care for a disease that has been associated with social stigma. Authors also note that the acceptability of data sharing and confidentiality is contingent upon the level of work invested in comprehending and resolving possible problems, as well as the establishment of confidence among stakeholders regarding the characteristics of the systems and their intended use [101]. This was similar to work that aimed at assessing participants' attitudes on privacy and security of medical technologies through focus groups and a standardized questionnaire survey [99]. The results of this analysis indicated that the incorporation of medical assistive technology in home environments is contingent upon the consideration of both security and privacy factors. Particularly, the examination of data about gender, health state, and age unveiled that females and individuals in good health exhibit a greater need for stringent security and privacy measures, in comparison to men and older individuals who are experiencing health issues [99]. Finally, one article used a triangular study including observations, focus groups, and exit interviews of a gradual EHR implementation [100]. Shield et al. found that the prioritization of patient trust in physicians and the establishment of secure physician-patient interactions seem to outweigh the majority of patients' apprehensions regarding information technology [100].

**4.2.3 Population Distribution.** As shown in Table 3, many of the 80 articles did not report population distribution of the participants (44.44%, 8) [8, 45–47, 51, 53–56, 58–68, 70–77, 79–90, 92–95, 99–101, 104–106, 108–112, 114–116, 118, 119, 122]. Most of the remainder studies were conducted in urban settings (37.5%, 6) [48, 49, 57, 78, 98, 117, 120], furthermore five studies were conducted in a rural setting [102, 103, 107, 121, 123], and six studies reported mixed populations [50, 52, 91, 96, 97, 113]. No articles reported on an exclusively suburban population setting.

**4.2.4 Study Population Setting.** Of the 80 user-focused articles, 20 focused exclusively on healthcare professionals, including medical doctors, nurses, and pharmacists [50, 54, 55, 60, 61, 63, 64, 72, 74, 75, 79, 84, 87, 88, 92, 94, 102, 103, 107, 119]. Furthermore, 13 articles studied patients and patient communities [8, 57, 58, 67, 76, 86, 89, 90, 98, 106, 110, 117, 123]. Additionally, six articles comprised of both healthcare professionals and patients [66, 100, 101, 111, 113, 120]. Similarly, six articles analyzed the perspectives of general hospital employees [69, 70, 73, 83, 118, 121] and only one article combined these participants with patients [93].

Seven articles studied non-medical experts such as IRB directors and information technology experts [53, 62, 81, 96, 104, 115, 122]; moreover, three articles studied both medical and non-medical experts [47, 77, 116]. On the other hand, only four articles recruited students for their studies [49, 78, 95, 108].

In addition to these studies, 15 articles studied the general public. However, in some articles, there were some conditions for the participants, such as a user of a specific technology or speaking a particular language [51, 52,

Table 4. Percentage and Number of Study Participants for Different User Studies

	Qual Studies (n = 17)	Quant Studies (n = 52)	Mixed-Methods (n = 11)
<b>Num Participants</b>			
> 0, ≤ 100	100% (17)	11.54% (6)	36.36% (4)
> 100, ≤ 500	0% (0)	40.38% (21)	45.45% (5)
> 500, ≤ 1000	0% (0)	23.08% (12)	0% (0)
> 1000, ≤ 5000	0% (0)	15.38% (8)	9.09% (1)
> 5000	0% (0)	5.77% (3)	9.09% (1)
Not reported	0% (0)	3.85% (2)	0% (0)

65, 71, 82, 97, 97, 99, 99, 105, 105, 109, 114, 114, 124]. In contrast, seven other articles did not determine the types of participants they recruited for their studies [46, 48, 56, 59, 91, 109, 112]. For these articles, we assumed that the participants were pooled from the general public.

**4.2.5 Study Geographical Location.** Out of the 80 studies, most studies were conducted in the US [8, 79–91, 100, 101, 103, 104, 110, 111, 114, 116, 118, 119, 122, 123]. The second most prominent region as Europe, where 21 studies took place [45, 46, 62–70, 95–99, 109, 112, 113, 115, 117]. Moreover, eight studies were conducted in the Middle East including Iran, Jordan, Israel, Qatar, Turkey, and Lebanon [48, 53–57, 105, 120], and eleven other studies were organized in other Asian countries such as India, Taiwan, China, Pakistan, South Korea, Indonesia, and Malaysia [47, 49, 59, 71–78]. Furthermore, four were conducted in the Oceania region, three of which [50, 51, 102] were in New Zealand and only one [52] in Australia. Only two studies were conducted in Africa, both in Nigeria [93, 107]. Similarly, only one study was conducted in South America; specifically, El Salvador [92], and two studies were transcontinental: the first one included Peru, South Africa, Thailand, and the US [106] and the second one included countries such as the US, France, and England [94]. Five studies did not specify the region where they conducted their studies [58, 60, 61, 108, 121].

**4.2.6 Number of Participants.** The most participants reported in qualitative studies is 87 participants [110], whereas the average number of participants in these studies is 31.83. However, we noticed that studies that employed focus groups had more participants on average (55.67) than interview-based studies. The least number of participants for qualitative studies was three [108]. As for mixed-method studies, the average number of participants is 259, whereas the maximum number of participants in one study is 1,031 and the minimum number of participants is 16. Furthermore, only one quantitative study did not report the number of participants. As such, the average number of participants for the rest of the quantitative studies is 1,215.46, and the maximum number of participants in a single study is 17,000. In contrast, the minimum number of participants is six.

**4.2.7 Regulatory Considerations.** Through our corpus, a discerning analysis reveals a nuanced landscape of HIPAA integration within the study design of user studies. Only five scholarly articles [72, 79, 81, 116, 118] adeptly integrated HIPAA issues into their study methodology, thoroughly exploring the perceptions, and understanding of HIPAA and discerning patterns of compliance with HIPAA regulations. These research publications are notable for their thorough investigations into the convergence of healthcare data privacy and security from the perspective of users, adeptly negotiating the complexities of HIPAA rules. One such study [81] investigates the practices of information security and analyzes the patterns of behaviors that are linked to enhanced regulatory compliance. The research conducted in this study identified three distinct groups, which have been labeled as leaders, followers, and laggards. These clusters have been determined based on the observed variance in security practice patterns. According to the authors, the clusters exhibit notable distinctions in non-technical practices as opposed to technical ones. Hospitals that used a balanced approach, encompassing both technical and non-technical practices, had the best degree of compliance. In contrast, a significant majority of

the remaining studies opted for a cautious approach when discussing regulatory frameworks, with seven articles [55, 56, 58, 84, 101, 104, 122] briefly addressing HIPAA and only two [112, 115] mentioning the **General Data Protection Regulation (GDPR)**. The references encompassed a spectrum of topics, including a brief acknowledgment of the regulatory framework's role in regulating healthcare data management, or a concise assessment of the subjects' adherence or lack thereof to the specified regulations.

**4.2.8 Card Sorting.** For the 26 articles most relevant to our subject matter, we conducted a card sorting exercise to reveal the specific human factor aspects studied thus far. Through this exercise, we identified a total of 12 labels about the human factors of information security in healthcare, namely: "Risk Perception," "Data Sharing," "EHR Interactions," "Risk Awareness," "Technology Adoption," "Regulatory Compliance," "Individual Differences," "Secure Communications," "Mobile Applications," "Social Influence," "Privacy," and "Contact Tracing." In the following sections, we have provided details of both the significant labels identified in this work and the user studies classified under each label. More details on these articles are available in Table 5 as well as Appendix A.

*Risk perception:* According to Zou et al. [125], risk perception is "a person's subjective assessment of the probability that a specific event happens and how concerned they feel about its consequences". However, 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 of healthcare data. Articles were categorized in the risk perception label when part of the study or its entirety explored participants' attitudes, impressions, and opinions on risks related to healthcare data. Risk perception was the most frequent label in our corpus where 61.54% of the articles were labeled within this category [46, 58, 62, 74, 80, 81, 83, 90, 91, 99, 106, 109, 111, 112, 114, 117]. The results of these articles show that participants have different perceptions of risk. Shnall et al. [111] claim that several participants perceived the mobile application being tested as risky and were apprehensive about data storage, leaks, and tracking. However, the participants also declared that these risks are inevitable.

On the other hand, 85% of participants in Giguere et al.'s study did not express any concerns about data privacy [106]. This study analyzed users' perception of the risk of using SMS for communication that consisted of several tiers of privacy-preserving safeguards, which may have caused the participants to express lower concern about data privacy. However, it was worrying to learn that few participants in the study declared passwords were obsolete, suggesting an underestimation of risk while interacting with a system misconceived to be privacy-preserving. These studies suggest that future work should further test how risk and privacy communication impact users' perception of healthcare systems.

*Data sharing:* Articles were classified within this label if they explored the subject of healthcare data use and sharing either with healthcare professionals for the purposes of examining patients and diagnosis or with the research community through healthcare information commons. The 14 articles [54, 62, 64, 68, 73, 90, 91, 97, 99, 106, 109, 114, 115, 121] generally aimed at understanding the perspective of participants on responsible data sharing practices that would be acceptable to the patients but also beneficial to the research communities. Similar results were found in these articles, which indicate that patients support data sharing as long as it allows for the greater good—it benefits the public, or in case the data is shared with a healthcare professional for personal health purposes. Nonetheless, people still have reservations about the privacy and confidentiality of sensitive data, data breaches, and bias.

*EHR:* Electronic healthcare records systems collect essential and private data about patients' medical history and the subsequent care they have received; as such, they store an extensive history of clinical information for each patient; not only that, they also contain personal information, such as demographics, billing data, and insurance information. As such, examining the users' perspective and understanding of such tools is very important to improve the security of EHR. In this regard, we found eight articles [58, 80, 81, 91, 97, 104, 115, 121] in our corpus pertaining to user interactions with EHR. These articles confirm through their results that the patients and the general public have concerns over privacy and security, and are prudent about using EHR technologies.



Table 5. Key Information about the Card Sorting Articles Including the Number of Participants, Location of Study, Population, Type of Study, and Labels

Ref	# Participants	Location	Population	Type of Study	Risk Perception	Data Sharing	EHR	Risk Awareness	Technology Adoption	Regulatory Compliance	Individual Differences	Secure Communications	Mobile Applications	Social Influence	Privacy	Contact tracing
[83]	397	USA		Online survey	●	–	–	●	–	–	●	–	–	–	–	–
[106]	187	Peru		Computer-assisted self-interview	●	●	–	–	–	–	–	●	●	–	–	–
[79]	131	USA		Survey	–	–	–	●	●	●	–	–	–	–	–	–
[81]	250	USA		Telephone survey	●	–	●	–	●	●	–	–	–	–	–	–
[74]	252	South Korea		Survey	●	–	–	●	–	–	–	–	–	–	–	–
[73]	93	China + Pakistan		Questionnaire	–	●	–	–	–	●	●	–	–	–	●	–
[54]	221	Jordan		Survey	–	●	–	●	–	–	●	–	–	●	–	–
[99]	19104	Germany		Focus group & Survey	●	●	–	–	●	–	–	–	–	–	–	–
[91]	1000	USA		Telephone Survey	●	●	●	–	–	–	–	●	–	–	–	–
[115]	14	Sweden & Italy & UK & Ireland & Australia	+  +  +	Semistructured interviews	–	●	●	–	●	–	–	–	–	–	–	–
[62]	773	Europe		Interviews or online questionnaires	●	●	–	–	●	–	●	–	–	–	–	–
[58]	117	†		Online Survey	●	–	●	–	●	–	–	–	–	●	–	●
[80]	394	USA		Mturk Survey	●	–	●	–	–	–	–	–	–	–	–	–
[90]	3516	USA		Online Questionnaire	●	●	–	–	–	–	●	–	–	–	–	–
[104]	133	USA		Survey	–	–	●	●	–	●	–	–	–	–	–	–
[112]	50	Italy + Greece + Ireland		Focus Groups	●	–	–	●	–	●	–	●	–	–	–	–
[121]	14	USA		Observation & interview	–	●	●	●	–	–	–	–	–	–	–	–
[46]	4357	Germany		Cross-sectional survey	●	–	–	–	●	–	–	●	–	–	–	●
[114]	75	USA		Community advisory panel	●	●	–	–	–	–	–	–	–	●	–	–
[109]	22	England		Focus Groups	●	●	–	–	–	–	–	–	–	–	–	–
[97]	80	England		Focus Groups	–	●	●	–	–	–	–	–	–	–	–	–
[111]	80	USA	+	Focus Groups	●	–	–	–	–	–	–	●	–	–	–	–
[68]	260	Germany & Switzerland		Survey	–	●	–	–	●	–	–	●	–	–	–	–
[72]	100	Indonesia	+  +  +	Online Survey	–	–	–	●	–	●	–	–	–	–	–	–
[64]	508	Switzerland		Questionnaire	–	●	–	–	–	●	–	●	–	–	●	–
[117]	15	Norway		Interview	●	–	–	–	–	–	–	●	–	–	●	–

Evaluation: ● = Label Detected; – = Label not Detected; † = not enough information.

Population: = Hospital privacy and security managers; = Hospital or Physician's Office Employees; = General Public; = Nurses; = Doctors; = Patients; = Technical Experts; = Pharmacists; = Healthcare providers.

Furthermore, it was determined that providers' reassurance and encouragement positively impact patients' continuous and systematic usage of patient portal software in general and lowers their security concerns [58].

**Risk Awareness:** Despite the abundant potentialities for cyber risk in the healthcare sector [126–128], there is a startling level of naiveté among some healthcare professionals. The results from the eight articles [54, 72, 74, 79, 83, 104, 112, 121] in our corpus relevant to risk awareness, show that the knowledge levels of healthcare professionals regarding patient privacy, confidentiality, and data sharing practices are average [54] or lower [72]. It is reasonable to posit that such low security and privacy awareness among healthcare users could lead to insecure behaviors such as password sharing, improper data handling, and in some cases, a complete absence of password use [121]. Finally, it was also observed that disregarding the risks and ignoring consequences can impede security [121].



*Technology Adoption:* Technology generally accounts for a substantial impact on human life, and these technologies have a central place in today's world. Some people adapted quickly, while others resisted these changes brought upon them through technological advancements. Adoption, however, is essential in the context of digital transformation to guarantee its success. Similarly, technology adoption in the healthcare domain is crucial to its development. In this regard, eight articles [46, 58, 62, 68, 79, 81, 99, 115] in our corpus examined factors and inspected participants' requirements that would improve user acceptance and adoption of some healthcare technologies. These articles report similar results. The results reveal that the security and privacy aspects bolster the acceptance and adoption of healthcare technologies.

*Regulatory Compliance:* Of the 26 articles in our corpus, seven [64, 72, 73, 79, 104, 112] studied the ethical and legal aspects of healthcare data management. These articles mainly assess the HIPAA compliance of participants, as well as the cybersecurity conditions and behavior of healthcare practitioners and organizations. Notably [64, 72, 112] all show that healthcare professionals' understanding and security awareness levels are lacking and, in all cases, were average or less than average. Furthermore, all of the studies in this label determined that there needs to be more policies and reinforcement of specific behaviors that can impede security.

*Individual Differences:* An article was labeled as *individual differences* if an analysis is done to compare results from different types of individuals or participants in general. This comparison can be based on experience level, hospital size, marriage status, country of origin, health status, or even gender. As such, we found seven articles [54, 62, 73, 81, 83, 90, 99] from our corpus that did this type of analysis. In particular, Wilkowska and Ziefle show that females and healthy adults expect and demand the highest security and privacy standards compared to males and the ailing elderly [99]. In a different study, Shrivastava et al. investigated the extent to which security policies impact health information interoperability at different levels within the same hospitals [62]. The outcomes showed that hospitals with regional and organizational level privacy regulations have 85% and 76% higher likelihood of undergoing semantic and organizational level problems, respectively. Furthermore, hospitals with one **electronic medical record (EMR)** used throughout the hospital are 53% and 43% less prone to technical and semantic problems, respectively, compared to hospitals with more than one EMR system.

*Secure Communications:* In the case of healthcare, secure communications are not just a matter of security and privacy, but they can also be a medical concern. According to the *Joint Commission Center for Transforming Healthcare*, "it has been estimated that 80 percent of serious medical errors involve miscommunication during the hand-off between medical providers. Most avoidable adverse events are due to the lack of effective communication." As such, it is critical to understand the need for secure communications specific to the healthcare sector, both from the patient's perspective and the healthcare professionals. Subsequently, we categorized five articles [64, 68, 106, 112, 117] from our corpus of 26 within this label. Most of these articles have similar results that show that patients still do not fully trust the existing communications technologies, except for Elger's study [64] where 85% of the participants had no privacy concerns regarding using a secure SMS system for private medical communications.

*Mobile Applications:* As of July 2022, there were over 54,000 healthcare mobile applications in the Google Play Store alone. These applications range from medical communication apps to applications that analyze medical data to give advice. As such, these apps have become more and more valuable in the monitoring and even delivery of healthcare [129]. However, only three articles [91, 106, 111] from our corpus were related to mobile applications. These articles evaluate users' perceptions of mobile health applications regarding privacy, security, and quality of care and analyze the factors contributing to patients' intentions of using mobile healthcare applications. The results of these articles were somewhat different, where Schnall et al. [111] found that the majority of their participants expressed concerns over privacy and trust of their sensitive healthcare data and the people who would have access to their healthcare data. On the other hand, both Giguere et al. [106] and Richardson and Ancker's [91] studies found that the majority of participants are unconcerned about privacy and confidentiality when using a mobile healthcare application.

*Social Influence:* Social influence is a type of pressure exerted by an individual or a group on a person to attempt to impose dominant norms. This influence causes the behaviors, attitudes, beliefs, opinions, or feelings of an individual or group to change as a result of contact with another individual or group. In this vein, three articles [54, 58, 114] in our corpus were categorized as social influence. These articles proved that participants were influenceable. Namely, Moqbel et al. [58] 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. A different angle to this category was participants' concerns about the repercussions of social influence on the security of healthcare data [114].

*Privacy:* There is an abundance of data circulating online, a considerable share of which can be considered private. This data has been at the center of attention, especially from big data analytics companies. This has helped increase the need for and recognition of privacy, including healthcare privacy. Most of the articles in our corpus touch upon privacy, but three of these articles [64, 73, 117] were directed exclusively towards the privacy of healthcare data. Accordingly, in their study Elger [64] assesses the knowledge and perceptions of physicians on healthcare data violations of privacy and confidentiality; through this study, the author found that barely 11% of the participants recognized all the confidentiality violations in the test cases they were presented with. On a different note, Tjora et al. examined and analyzed the usability and experiences of patients using a secure patient-physician communication system compared to their privacy expectations and perceptions of this systems [117]. The results show that although participants were not too concerned about privacy, they still avoided using the system for "intimate details."

*Contact Tracing:* Out of the 26 articles in our corpus, only two [46, 58] were categorized as contact tracing. Contact tracing is identifying and evaluating people who have been in contact with an infectious disease to prevent it from being transmitted further. Contact tracing is critical in the fight against epidemics since it helps limit the number of infections. However, with the emergence of digital contact tracing applications, users have expressed privacy and security concerns [130]. These concerns stem from apprehension of data breaches or having their data collected by government entities [131]. However, this did not deter participants from approving COVID-19 contact tracing apps and recognizing the importance of these applications in the right circumstances. Kozyreva et al. [46] showed that the acceptability of privacy-encroaching measures across the four waves of COVID-19 in Germany was correlated with the participants' risk perceptions of the pandemic.

## 5 IMPLICATIONS

The contributions of previous works in enhancing the privacy and security of sensitive patient data are evident and commendable. However, a more comprehensive exploration is required to fully grasp the intricacies and challenges associated with healthcare security and privacy. Our study reviewed articles from diverse global regions, each subject to different cybersecurity and healthcare norms and regulations. While compliance frameworks—exemplified by the **Health Insurance Portability and Accountability Act (HIPAA)**—set the baseline for regulatory requirements and data protection, the true essence of adequate security and privacy often extends beyond these legal boundaries. Furthermore, our analysis reveals a significant omission of numerous global privacy regulations concerning health-related data.

### 5.1 Proactive Healthcare Security Approach

The dynamic nature of users, for whom security or privacy might not always be a primary concern, mandates further research to discern motivations behind control circumvention, particularly regarding sensitive patient data. Our analysis discerns three predominant themes related to the human-centric challenges in healthcare information security: Inconsistent access controls; Modes of communication that do not adhere to compliance or are inherently insecure; Disruptive policies for updates and data backups. Prior works concerning human interactions in healthcare predominantly revolved around understanding circumvention behaviors related

to authentication [132]. A notable observation is the rampant sharing of login credentials among providers, attributed to inconsistent access control policies [112, 121].

In our analysis, we found that healthcare access control paradigms often lack the foresight of individualistic provider needs or the diverse range of tasks they perform daily. Typically modeled in hierarchical tiers, senior providers are bestowed with maximal privileges, whereas their junior counterparts and other staff members navigate with restricted access [70, 112, 121]. Such restrictions, although designed for data security, ironically result in credential sharing especially when immediate access is indispensable for critical patient care or when the intended user is yet to undergo necessary training [5]. Supplementing this, existing literature also underscores recurrent password-related challenges, from the adoption of weak passwords to prolonged machine inactivity. Although access control cards serve as an antidote to some of these issues, they fall short in addressing the more profound circumvention challenges [62].

## 5.2 Policy Compliance

A salient theme in our analysis pertains to the secure communication, or the evident lack thereof, between healthcare professionals and patients. A subset of the literature indicates that providers frequently resort to messaging platforms not compliant with HIPAA regulations for disseminating test results to patients and peers [112, 120]. Interestingly, patients expressed an inclination towards conventional e-mail over HIPAA-approved secure messaging, citing the latter's complexity as a deterrent. Instances abound where providers share diagnostic images with patients via WhatsApp, a widely used messaging platform owned by Meta. This behavior might emanate from misplaced trust in such platforms, which often publicize their end-to-end encryption capabilities. Further inquiry is imperative to comprehend the hurdles associated with leveraging acknowledged, HIPAA-compliant messaging systems, such as American Messaging, to facilitate secure dialogue among providers and between providers and patients.

Another theme emerging from our study revolves around the dilemmas of administering security updates and instigating automatic backups. A common grievance among providers is the untimely manifestation of these updates, often during patient interactions [112]. Delving deeper to discern an updated schedule that is both swift and minimally intrusive to the providers' workflow is crucial. It is noteworthy that technologies such as encryption [133], blockchain [134], cloud computing [135], and access controls [136] frequently surface in scholarly discourse. While these technologies undeniably pave the path for prospective avenues and challenges in healthcare, there exists a palpable disconnect between their theoretical promise and current applicability. Their exaggerated representation in academic works risks eclipsing critical discussions on present-day security and privacy practices. The introduction of innovative technologies in the healthcare domain is inherently sluggish, largely attributed to stringent legal and compliance mandates. Nevertheless, while keeping an eye on emerging technologies, it is paramount to also spotlight promising technical solutions already at our disposal. For example, continuous authentication mechanisms leveraging biometrics or hardware tokens could empower healthcare personnel to secure computing devices based on the proximate presence of an authorized user [137]. Insights derived from user studies indicate the potential advantages of such automated security features, echoing the efficacy of automated software updates.

## 5.3 Focus on Private and Allied Practices

Our analysis revealed that the majority of the surveyed literature predominantly centers around hospitals and substantial medical institutions [81]. It is paramount to note that such environments, though substantial, offer only a limited glimpse into the comprehensive panorama of healthcare workspaces, especially since different organizations have different resource limitations when it comes to technological usage. The unique nature of hospitals is underscored by their abundant access to resources, ensuring robust measures to enforce, implement, and monitor privacy and security protocols. This financial muscle facilitates more substantial investments in security apparatuses, the fostering of a proactive organizational security culture, and dedicated technical

assistance. Consequently, issues that arise in hospitals, and their corresponding remedies, should be cautiously extrapolated to broader medical contexts.

A recurrent theme in healthcare literature is the prioritization of patient well-being above all other objectives, relegating security and privacy concerns to secondary importance [79]. Small-scale health enterprises, often operating under tight financial constraints, find it particularly challenging to allocate resources to these secondary objectives [54]. Such entities are in dire need of guidance to optimize their expenditures and effectively implement privacy and security measures. In this light, the academic community holds a crucial responsibility to address the most salient challenges as a priority. An enlightening study by Dykstra et al. delves into the cybersecurity landscape of private practice audiology clinics. The study underscores expertise, time, and financial limitations as the principal barriers to enhancing cybersecurity standards [79]. Although these challenges are prevalent across many sectors, they demand distinct attention and recognition within the healthcare domain. For instance, in the event of a technical issue at a clinic, a solo practitioner might bypass a sanctioned telehealth system in favor of an unauthorized personal device. Thus, there is a pressing need for further research to delve into and analyze these nuanced situations, with a focus on private practices and other healthcare institutions facing resource constraints.

Furthermore, the realm of allied healthcare, encompassing disciplines like audiology, optometry, occupational therapy, and physical therapy, often remains underrepresented in security and privacy research. This oversight is a significant gap for several reasons: *Sensitive Patient Data*: Like mainstream medicine, allied healthcare professionals collect and manage a vast array of sensitive patient information. This data ranges from detailed medical histories to diagnostic results and rehabilitation plans. Any breach in these systems could lead to significant patient harm, both medically and in terms of privacy violations. *Interconnected Systems*: The integrated nature of healthcare today means that many allied health professionals interface with broader medical systems. For instance, an optometrist might share data with an ophthalmologist or a general practitioner. This interconnectivity introduces multiple potential entry points for cyber threats, increasing the overall vulnerability of the healthcare network. *Diverse Technology Integration*: Many allied healthcare disciplines have embraced modern technologies for diagnostics, treatment planning, and patient management. Each piece of technology, from specialized diagnostic equipment to bespoke software platforms, introduces its own set of security challenges. *Resource Constraints*: Similar to private practices in mainstream medicine, many allied health clinics operate as small businesses with limited financial and technical resources. They might lack dedicated IT departments or robust cybersecurity measures, making them potentially more susceptible to breaches. Given these complexities, it is paramount for the research community to prioritize the examination of privacy and security measures within allied healthcare. An integrated approach, considering the unique challenges and strengths of these disciplines, will be crucial in creating a holistic and fortified healthcare data protection framework.

#### 5.4 Studies in Rural Setting and Developing Nations

Rural settings and developing nations present a complex tapestry of healthcare challenges, deeply entwined with their socio-economic, technological, and infrastructural landscapes [102, 107]. The prevailing narrative in healthcare security and privacy research, however, seems to marginalize these locales, despite their distinctive vulnerabilities and challenges. It is crucial to highlight that these areas often grapple with not just financial constraints but also issues like limited technical expertise, inadequate training programs, outdated technology infrastructure, and sometimes even basic challenges such as intermittent power supplies or lack of reliable internet connectivity [121]. These myriad factors further compound their vulnerabilities to security and privacy threats.

Our article and analysis underscore a conspicuous gap: the absence of detailed risk assessment and vulnerability analyses tailored to these contexts. Such granular analyses are instrumental in allowing these resource-strapped organizations to discern, evaluate, and strategically prioritize their security and privacy initiatives. One promising avenue for these regions could be to harness economic models tailored for resource

optimization. The Gordon–Loeb model, for instance, provides a framework for determining the optimal amount to invest in information security [138]. Leveraging such models, rural and developing settings can ensure that every dollar spent yields maximal security benefits. Furthermore, the formulation and enforcement of cybersecurity policies in these settings demand a delicate balance. While rigorous security protocols are essential, it is equally vital to ensure that these policies are implementable given the ground realities and do not inadvertently stifle essential medical services. Economic research that elucidates the tradeoffs involved, quantifies attacker motivations and strategizes ways to confound and thwart malevolent actors can be invaluable in this context. Additionally, collaborative efforts that involve international organizations, cybersecurity experts, and local stakeholders could pave the way for creating robust, context-aware security frameworks that respect local nuances while offering world-class protection.

### 5.5 Understanding the Patient’s Perspective

Throughout the user studies we reviewed, there emerged a dominant theme centered on discerning patients’ risk perceptions alongside the security behaviors exhibited by healthcare professionals [83, 114, 121]. Surprisingly, there appeared to be a lack of in-depth investigations into the levels of privacy awareness among patients, as well as their adherence to, and understanding of, confidentiality measures. This is concerning since security and privacy frameworks ought to be tailored with a strong consideration of patients’ preferences and perspectives regarding their data.

Patients stand at the forefront of the healthcare ecosystem and bear the immediate brunt of any security breaches. Their data, containing sensitive personal and medical information, is not just a trove of intimate knowledge but also represents their vulnerabilities. Hence, the sanctity of this data is of paramount importance. Research endeavors should not only identify but also bridge the apparent gaps in patients’ understanding of the potential consequences of security breaches. Such breaches can have wide-ranging implications, from personal repercussions to broader societal impacts. Additionally, it is essential to delve deeper into patients’ grasp of the intricacies of healthcare privacy and confidentiality standards. How informed are they about their rights, and how comfortable do they feel navigating the complex landscape of data protection? Furthermore, the critical aspect of any healthcare system is trust [139]. In this context, gauging the quantum of trust patients repose in their healthcare institutions becomes critical [97]. Do they believe in the institution’s ability and intention to shield their data from malicious threats? Are they confident about the efficacy of the security protocols in place, and do they feel adequately informed about them? Exploring these avenues will provide insights that can guide the creation of more holistic and patient-centric security strategies [140].

### 5.6 Education and Training

Our analysis of user studies revealed a palpable need for more bespoke security and privacy awareness education catered to healthcare professionals and ancillary staff. The rigorous and specialized training that healthcare professionals undergo to improve their teamwork and patient care skills should be mirrored in their cybersecurity training. With the ever-growing landscape of security threats to patient privacy and data, the emphasis on continuous, scenario-based education is more pressing than ever. A particular area of concern that repeatedly emerged was the domain of data sharing and secure communications. These realms are often the battlegrounds where the skirmishes between ease-of-use and security play out. As such, security awareness curricula for healthcare must prioritize the elucidation of threats associated with data-in-transit. The aim should be twofold: to raise awareness about potential pitfalls and to foster habits that facilitate secure communication between healthcare professionals.

However, merely increasing awareness does not suffice. An essential aspect of training involves aligning healthcare professionals’ risk perceptions with the actual risks intrinsic to the realm of patient data security and privacy [81]. This alignment is critical, as there are potential pitfalls associated with both ends of the risk perception spectrum [121]. On one end, hyperbolized, fear-driven training can lead to an inflated sense of risk,



which may paradoxically deter professionals from adhering to recommended security protocols, or worse, lead to operational paralysis [141]. On the other extreme, training content riddled with technical jargon, lacking in the medical context, or not tailored to the healthcare setting can alienate professionals, rendering the exercise futile [142, 143]. Recent academic discourse advocates for a shift towards a more immersive, simulation-driven approach to security awareness training, drawing parallels from real-world scenarios encountered in healthcare environments of varying scales. Such simulation-based modules can ensure that the training remains both contextually relevant and engaging, leading to better retention and application [144]. Notably, our article underscored a glaring absence of such comprehensive, realistic training programs, pointing towards an area for future exploration and development.

## 6 LIMITATIONS AND FUTURE WORK

Healthcare is a broad and diverse sector with many niche journals and publications. Despite our best efforts, we may have missed essential contributions reported in publications for medical sub-specialties published in paid venues or otherwise excluded by our search criteria. Future work is needed to understand when, how, and why healthcare workers circumvent compliant workflows and tools. Prior work has been focused primarily on authentication-related circumvention and usability, and a broader examination is warranted. Furthermore, past research has drawn heavily from surveys so that in-site data would provide further grounding and accuracy.

## 7 CONCLUSION













The healthcare sector is increasingly digitized; however, with technological interventions, privacy risks and security concerns about data storage, access, and transfer have increased significantly for telehealth. The question remains about how the research community addresses these concerns from the technical and user perspectives. To understand this issue further, we conducted a detailed systematic literature review. We collected 5,520 articles and analyzed 1,553 peer-reviewed research articles published and available over seven digital spaces: ACM DL, Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. These articles examined the privacy, security, and risk postures of patient data in healthcare organizations. We found that current research focuses primarily on data encryption and frameworks while understudying the user risk perspective of privacy and security. Along with the socio-technical component of healthcare privacy and security, it was concerning to note that < 9% of the articles conducted any user studies. Among those, the studies were influenced by survey designs rather than in-depth, longitudinal user-focused studies. Additionally, these studies focused on more extensive settings by severely ignoring the organizations with limited resources, such as the private healthcare sector. We conclude with actionable recommendations from the rich literature we studied that can enhance the privacy and security aspects of the healthcare sector and provide future directions to address these gaps.



## APPENDIX

## A OVERVIEW OF SECURITY-FOCUSED USER STUDIES

Table 6. 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 Awareness,  = Tech Adoption,  = Social Influence,  = Risk Perception,  = Mobile Healthcare,  = Privacy,  = Contact tracing

Study	Goal	Methods	Principal Findings	Labels
[83]	Understand reasons why hospital employees click on phishing e-mails	Quantitative: partial least squared structural equation modeling	Workload has a significant negative effect on secure behavior	  
[106]	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	   
[79]	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	  
[81]	Assess security practices of healthcare organizations	Quantitative: Ward's cluster analysis using minimum variance	Participating hospitals were clustered into three clusters: leaders, followers, and laggards Hospitals prioritize technical security solutions and data privacy over security management processes and performing regular audits	    
[74]	Assess nurses' <b>health information security (HIS)</b> 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 ( $estimate = 0.515, p < 0.001$ )	 
[73]	Evaluate the extent to which access to <b>patients' physiological parameters (PPP)</b> 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	   
[54]	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	   




















(Continued)

Table 6. Continued

Study	Goal	Methods	Principal Findings	Labels
[99]	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	   
[91]	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%)	   
[115]	Evaluate the perceptions of experts on using ML-based <b>privacy enhancing technologies (PETs)</b> 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	  
[62]	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 <b>technical interoperability (TI)</b> issues. Hospitals using one EMR are 53% less like to encounter TI issues compared with hospitals using numerous EMR systems	   
[58]	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	     *** faMap-Marked
[80]	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.	 
[90]	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)

Table 6. Continued

Study	Goal	Methods	Principal Findings	Labels
[104]	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	  
[112]	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	  
[121]	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	   
[46]	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.	  *** faMap-Marked
[114]	Investigate the public's perceptions about the important concerns in the design of <b>medical information commons (MIC)</b>	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	  
[109]	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.	 
[97]	Investigate the participants' perceptions on healthcare data sharing process and establishing ways to gain their trust of the process	Sequential mixed methods: Thematic analysis for qualitative data and descriptive statistics for quantitative data	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	 

(Continued)

Table 6. Continued

Study	Goal	Methods	Principal Findings	Labels
[111]	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	 
[68]	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	  
[72]	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)	 
[64]	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	   
[117]	Analyze the privacy posture of patients who use secure <b>electronic communication systems (ECS)</b> 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	 

## ACKNOWLEDGMENTS

We thank the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Laboratory at the University of Denver. We would also like to thank Salman Hosain for their initial contribution to this research. Any opinions, results, conclusions, or recommendations stated in this material are exclusively those of the writers and may not necessarily represent the perspectives of the University of Denver, the University of Washington, and the Designer Security.

## REFERENCES

- [1] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. 2019. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* 19, 2 (2019), 326.
- [2] Beth Ann Savage. 2017. *A Qualitative Exploration of the Security Practices of Registered Nurses*. Ph.D. Dissertation. Walden University.
- [3] Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 25, 1 (2017), 1–10.
- [4] Muneeb Ahmed Sahi, Haider Abbas, Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A. Orgun, Waseem Iqbal, Imran Rashid, and Asif Yaseen. 2017. Privacy preservation in e-healthcare environments: State-of-the-art and future directions. *IEEE Access* 6 (2017), 464–478.
- [5] Lynne Coventry and Dawn Branley. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* 113 (2018), 48–52.

- [6] Albese Demjaha, Tristan Caulfield, M. Angela Sasse, and David Pym. 2019. 2 fast 2 secure: A case study of post-breach security changes. In *Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, IEEE, Stockholm, Sweden, 192–201.
- [7] William J. Gordon, Adam Wright, Ranjit Aiyagari, Leslie Corbo, Robert J. Glynn, Jigar Kadakia, Jack Kufahl, Christina Mazzone, James Noga, Mark Parkulo, et al. 2019. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open* 2, 3 (2019), e190393–e190393.
- [8] David A. Haggstrom, Jason J. Saleem, Alissa L. Russ, Josette Jones, Scott A. Russell, and Neale R. Chumbler. 2011. Lessons learned from usability testing of the VA’s personal health record. *Journal of the American Medical Informatics Association* 18, Supplement\_1 (2011), i13–i17.
- [9] Axel Wirth. 2020. Cyberinsights: COVID-19 and what it means for cybersecurity. *Biomedical Instrumentation and Technology* 54, 3 (2020), 216–219.
- [10] Gültekin Altuntaş, Fatih Semerciöz, and Hanife Eregez. 2013. Linking strategic and market orientations to organizational performance: The role of innovation in private healthcare organizations. *Procedia-Social and Behavioral Sciences* 99 (2013), 413–419.
- [11] Álvaro S. Almeida. 2017. The role of private non-profit healthcare organizations in NHS systems: Implications for the Portuguese hospital devolution program. *Health Policy* 121, 6 (2017), 699–707.
- [12] Tasneem Majam and Francois Theron. 2006. The purpose and relevance of a scientific literature review: A holistic approach to research. *Journal of Public Administration* 41, 3 (2006), 603–615.
- [13] Hilda Hadan, Nicolas Serrano, Sanchari Das, and L Jean Camp. 2019. Making IoT worthy of human trust. In *Proceedings of the TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*. Washington College of Law, Washington, DC, 12.
- [14] Sanchari Das. 2020. *A Risk-reduction-based Incentivization Model for Human-centered Multi-factor Authentication*. Ph.D. Dissertation. Indiana University.
- [15] Ellen W. Clayton, Colin M. Halverson, Nila A. Sathe, and Bradley A. Malin. 2018. A systematic literature review of individuals’ perspectives on privacy and genetic information in the United States. *PLOS One* 13, 10 (2018), e0204417.
- [16] Alaa A. Abd-Alrazaq, Bridgette M. Bewick, Tracey Farragher, and Peter Gardner. 2019. Factors that affect the use of electronic personal health records among patients: A systematic review. *International Journal of Medical Informatics* 126 (2019), 164–175.
- [17] Clemens Scott Kruse, Darcy A. Argueta, Lynsey Lopez, and Anju Nair. 2015. Patient and provider attitudes toward the use of patient portals for the management of chronic disease: A systematic review. *Journal of Medical Internet Research* 17, 2 (2015), e3703.
- [18] Mohammad S. Jalali, Sabina Razak, William Gordon, Eric Perakslis, and Stuart Madnick. 2019. Health care and cybersecurity: Bibliometric analysis of the literature. *Journal of Medical Internet Research* 21, 2 (2019), e12644.
- [19] Sokratis Nifakos, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* 21, 15 (2021), 5119.
- [20] Shilan S. Hameed, Wan Haslina Hassan, Liza Abdul Latiff, and Fahad Ghabban. 2021. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science* 7 (2021), e414.
- [21] Bakheet Aljedaani and M. Ali Babar. 2021. Challenges with developing secure mobile health applications: Systematic review. *JMIR mHealth and uHealth* 9, 6 (2021), e15654.
- [22] Katarzyna Kolasa, Francesca Mazzi, Ewa Leszczuk-Czubkowska, Zsombor Zrubka, and Márta Péntek. 2021. State-of-the-art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review. *JMIR mHealth and uHealth* 9, 6 (2021), e23250.
- [23] Valerie J. M. Watzlaf, Leming Zhou, Dilhari R. DeAlmeida, and Linda M. Hartman. 2017. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers. *International Journal of Telerehabilitation* 9, 2 (2017), 39.
- [24] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G. Altman, and PRISMA Group\*. 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine* 151, 4 (2009), 264–269.
- [25] Elizabeth Stowell, Mercedes C. Lyson, Herman Saksono, René C. Wurth, Holly Jimison, Misha Pavel, and Andrea G. Parker. 2018. Designing and evaluating mHealth interventions for vulnerable populations: A systematic review. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal, Canada, 1–17.
- [26] Sanchari Das, Andrew Kim, Zachary Tingle, and Christena Nippert-Eng. 2019. All about phishing exploring user research through a systematic literature review. In *Proceedings of the 13th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2019)*. Springer, Nicosia, Cyprus, 10.
- [27] Sanchari Das, Bingxing Wang, Zachary Tingle, and L. Jean Camp. 2019. Evaluating user perception of multi-factor authentication: A systematic review. In *Proceedings of the 13th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2019)*. Springer, Nicosia, Cyprus, 10.
- [28] Naheem Noah and Sanchari Das. 2021. Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. *Computer Animation and Virtual Worlds* 32, 3-4 (2021), e2020.

- [29] John M. Jones, Reyhan Duezguen, Peter Mayer, Melanie Volkamer, and Sanchari Das. 2021. A literature review on virtual reality authentication. In *Proceedings of the 15th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2021)-Virtual Conference*. Springer, Virtual, 10.
- [30] Ritajit Majumdar and Sanchari Das. 2021. SOK: An evaluation of quantum authentication through systematic literature review. In *Proceedings of the Workshop on Usable Security and Privacy (USEC)*. Internet Society, Auckland, New Zealand, 10.
- [31] Faiza Tazi, Sunny Shrestha, Junibel De La Cruz, and Sanchari Das. 2022. Sok: An evaluation of the secure end user experience on the dark net through systematic literature review. *Journal of Cybersecurity and Privacy* 2, 2 (2022), 329–357.
- [32] Vibhor Gupta and Garima Metha. 2018. Medical data security using cryptography. In *Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science and Engineering (Confluence)*. IEEE, IEEE, Noida, India, 866–869.
- [33] Luca Brunese, Francesco Mercaldo, Alfonso Reginelli, and Antonella Santone. 2019. A blockchain based proposal for protecting healthcare systems through formal methods. *Procedia Computer Science* 159 (2019), 1787–1794.
- [34] Yu Tian, Yong Shang, Dan-Yang Tong, Sheng-Qiang Chi, Jun Li, Xiang-Xing Kong, Ke-Feng Ding, and Jing-Song Li. 2018. POPCORN: A web service for individual PrognOsis prediction based on multi-center clinical data CollabORatioN without patient-level data sharing. *Journal of Biomedical Informatics* 86 (2018), 1–14.
- [35] Geethapriya Thamilarasu and Christopher Lakin. 2017. A security framework for mobile health applications. In *Proceedings of the 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE, Prague, Czech Republic, 221–226. DOI : <http://dx.doi.org/10.1109/FiCloudW.2017.96>
- [36] Ahmed Ibrahim, Baban Mahmood, and Mukesh Singhal. 2016. A secure framework for sharing electronic health records over clouds. In *Proceedings of the 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH)*. IEEE, Orlando, FL, 1–8. DOI : <http://dx.doi.org/10.1109/SeGAH.2016.7586273>
- [37] Mutaz Zalloum and Hosam Alamleh. 2020. Privacy preserving architecture for healthcare information systems. In *Proceedings of the 2020 IEEE International Conference on Communication, Networks and Satellite (Commnetsat)*. IEEE, Batam, Indonesia, 429–432. DOI : <http://dx.doi.org/10.1109/Commnetsat50391.2020.9328985>
- [38] Ji Jia, Jinyang Yu, Raghavendra Sirigeri Hanumesh, Stephen Xia, Peter Wei, Hyunmi Choi, and Xiaofan Jiang. 2018. Intelligent and privacy-preserving medication adherence system. *Smart Health* 9-10 (2018), 250–264. DOI : <http://dx.doi.org/10.1016/j.smhl.2018.07.012>
- [39] Steven Walker-Roberts, Mohammad Hammoudeh, and Ali Dehghantanha. 2018. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access* 6 (2018), 25167–25177.
- [40] M. Paksuniemi, Hannu Sorvoja, Esko Alasaarela, and Risto Myllyla. 2006. Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit. In *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. IEEE, IEEE, Shanghai, China, 5182–5185.
- [41] Cliff X. Wang. 1999. Security issues to tele-medicine system design. In *Proceedings of the IEEE Southeastcon'99. Technology on the Brink of 2000 (Cat. No. 99CH36300)*. IEEE, IEEE, Lexington, Kentucky, 106–109.
- [42] Emmanouil G. Spanakis, Silvia Bonomi, Stelios Sfakianakis, Giuseppe Santucci, Simone Lenti, Mara Sorella, Florin D. Tanasache, Alessia Palleschi, Claudio Ciccotelli, and Vangelis Sakkalis. 2020. Cyber-attacks and threats for healthcare—a multi-layer thread analysis. In *Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, IEEE, Virtual, 5705–5708.
- [43] Kate Lopatina, V. A. Dokuchaev, and V. V. Maklachkova. 2021. Data risks identification in healthcare sensor networks. In *Proceedings of the 2021 International Conference on Engineering Management of Communication and Technology (EMCTECH)*. IEEE, IEEE, Vienna, Austria, 1–7.
- [44] Andrejs Romanovs, Edgars Sultanovs, Egons Buss, Yuri Merkuryev, and Ginta Majore. 2021. Challenges and solutions for resilient telemedicine services. In *Proceedings of the 2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. IEEE, IEEE, Vilnius, Lithuania, 1–7.
- [45] Serena Luchenski, Anjali Balasanthiran, Cicely Marston, Kaori Sasaki, Azeem Majeed, Derek Bell, and Julie E. Reed. 2012. Survey of patient and public perceptions of electronic health records for healthcare, policy and research: Study protocol. *BMC Medical Informatics and Decision Making* 12, 1 (2012), 1–6.
- [46] Anastasia Kozyreva, Philipp Lorenz-Spreen, Stephan Lewandowsky, Paul M. Garrett, Stefan M. Herzog, Thorsten Pachur, and Ralph Hertwig. 2021. Psychological factors shaping public responses to COVID-19 digital contact tracing technologies in Germany. *Scientific Reports* 11, 1 (2021), 1–19.
- [47] Jeongeun Kim and David W. Bates. 2011. Analysis of the definition and utility of personal health records using Q methodology. *Journal of Medical Internet Research* 13, 4 (2011), e1781.
- [48] Gonul Bodur, Secim Gumus, and Nazli Gul Gursay. 2019. Perceptions of Turkish health professional students toward the effects of the internet of things (IOT) technology in the future. *Nurse Education Today* 79 (2019), 98–104.
- [49] Kim Geok Chan, Saloma Pawi, Mei Fong Ong, Yanika Kowitlawakul, and Siew Ching Goy. 2020. Simulated electronic health documentation: A cross-sectional exploration of factors influencing nursing students' intention to use. *Nurse Education in Practice* 48 (2020), 102864.



- [50] Felicity Goodyear-Smith, Andy Wearn, Hans Everts, Peter Huggard, and Joan Halliwell. 2005. Pandora's electronic box: GPs reflect upon e-mail communication with their patients. *Journal of Innovation in Health Informatics* 13, 3 (2005), 195–202.
- [51] Inga M. Hunter, Richard J. Whiddett, Anthony C. Norris, Barry W. McDonald, and John A. Waldon. 2009. New Zealanders' attitudes towards access to their electronic health records: Preliminary results from a national study using vignettes. *Health Informatics Journal* 15, 3 (2009), 212–228.
- [52] Cameryn C. Garrett, Jane Hocking, Marcus Y. Chen, Christopher K. Fairley, and Maggie Kirkman. 2011. Young people's views on the potential use of telemedicine consultations for sexual health: Results of a national survey. *BMC Infectious Diseases* 11, 1 (2011), 1–11.
- [53] Rania Daraghmeah and Raymond Brown. 2021. A big data maturity model for electronic health records in hospitals. In *Proceedings of the 2021 International Conference on Information Technology (ICIT)*. IEEE, IEEE, Amman, Jordan, 826–833.
- [54] Reema Karasneh, Abdel-Hameed Al-Mistarehi, Sayer Al-Azzam, Sawsan Abuhammad, Suhaib M. Muflih, Sahar Hawamdeh, and Kareem H. Alzoubi. 2021. Physicians' knowledge, perceptions, and attitudes related to patient confidentiality and data sharing. *International Journal of General Medicine* 14 (2021), 721.
- [55] Edward Barayev, Omri Shental, Dotan Yaari, Elchanan Zloczower, Itai Shemesh, Michael Shapiro, Elon Glassberg, and Racheli Magnezi. 2021. WhatsApp Tele-Medicine—usage patterns and physicians views on the platform. *Israel Journal of Health Policy Research* 10, 1 (2021), 1–9.
- [56] Akram Farhadi and Maryam Ahmadi. 2013. The information security needs in radiological information systemsan insight on state hospitals of iran, 2012. *Journal of Digital Imaging* 26, 6 (2013), 1040–1044.
- [57] Issam Shaarani, Hussein Berjaoui, Alaa Daher, Mayar Khalil, Abed El Rahman Al Rifai, Radwan Saati, and Jumana Antoun. 2019. Attitudes of patients towards digital information retrieval by their physician at point of care in an ambulatory setting. *International Journal of Medical Informatics* 130 (2019), 103936.
- [58] Murad Moqbel, Barbara Hewitt, Fiona Fui-Hoon Nah, and Rosann M. McLean. 2021. Sustaining patient portal continuous use intention and enhancing deep structure usage: Cognitive dissonance effects of health professional encouragement and security concerns. *Information Systems Frontiers* 24, 5 (2021), 1–14.
- [59] Widia Resti Fitriani, Arief Fadli Wicaksono, Danang Gagastama Joewono, Muhammad Zidane Zaffar, Reza Akbar Shahputra, Ziegggy Ronnavelly, Achmad Nizar Hidayanto, and Lim Yohanes Stefanus. 2020. The antecedents of trust and their influence on M-health adoption. In *Proceedings of the 2020 5th International Conference on Informatics and Computing (ICIC)*. IEEE, IEEE, Virtual, 1–6.
- [60] Kathleen E. Walsh, Jessica L. Secor, Jon S. Matsumura, Margaret L. Schwarze, Beth E. Potter, Peter Newcomer, Michael K. Kim, and Christie M. Bartels. 2018. Promoting secure provider-to-provider communication with electronic health record messaging: An educational outreach study. *Journal for Healthcare Quality* 40, 5 (2018), 283.
- [61] Yong Sauk Hau, Jae Min Lee, Jaechan Park, and Min Cheol Chang. 2019. Attitudes toward blockchain technology in managing medical information: Survey study. *Journal of Medical Internet Research* 21, 12 (2019), e15870.
- [62] Utkarsh Shrivastava, Jiahe Song, Bernard T. Han, and Doug Dietzman. 2021. 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* 148 (2021), 104401.
- [63] Claudio Vitari and Roxana Ologeanu-Taddei. 2018. The intention to use an electronic health record and its antecedents among three different categories of clinical staff. *BMC Health Services Research* 18, 1 (2018), 1–9.
- [64] Bernice S. Elger. 2009. Violations of medical confidentiality: Opinions of primary care physicians. *British Journal of General Practice* 59, 567 (2009), e344–e352.
- [65] Ala Sarah Alaqra and Bridget Kane. 2020. Wearable devices and measurement data: An empirical study on ehealth and data sharing. In *Proceedings of the 2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)*. IEEE, Virtual, 443–448.
- [66] Terry Porteous, Christine Bond, Roma Robertson, Philip Hannaford, and Ehud Reiter. 2003. Electronic transfer of prescription-related information: Comparing views of patients, general practitioners, and pharmacists. *The British Journal of General Practice* 53, 488 (2003), 204.
- [67] Cherry Bartlett, Keith Simpson, and A. Neil Turner. 2012. Patient access to complex chronic disease records on the Internet. *BMC Medical Informatics and Decision Making* 12, 1 (2012), 1–7.
- [68] Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow. 2016. Improving individual acceptance of health clouds through confidentiality assurance. *Applied Clinical Informatics* 7, 04 (2016), 983–993.
- [69] Dimitris Gritzalis, A. Tomaras, S. Katsikas, and J. Keklikoglou. 1991. Data security in medical information systems: The Greek case. *Computers and Security* 10, 2 (1991), 141–159.
- [70] Dimitris Gritzalis, S. Katsikas, J. Keklikoglou, and A. Tomaras. 1992. Determining access rights for medical information systems. *Computers and Security* 11, 2 (1992), 149–161.
- [71] Dira Ayu Meigasari, Putu Wuri Handayani, Achmad Nizar Hidayanto, and Dumilah Ayuningtyas. 2020. Do electronic personal health records (E-PHR) influence people behavior to manage their health?. In *Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech)*. IEEE, IEEE, Bandung, Indonesia, 482–487.

- [72] Kalamullah Ramli. 2021. HIPAA-based analysis on the awareness level of medical personnel in indonesia to secure electronic protected health information (ePHI). In *Proceedings of the 2021 IEEE International Conference on Health, Instrumentation and Measurement, and Natural Sciences (InHeNce)*. IEEE, IEEE, Medan, Indonesia, 1–6.
- [73] Isma Masood, Yongli Wang, Ali Daud, Naif Radi Aljohani, and Hassan Dawood. 2018. Privacy management of patient physiological parameters. *Telematics and Informatics* 35, 4 (2018), 677–701.
- [74] EunWon Lee and GyeongAe Seomun. 2021. Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *International Journal of Environmental Research and Public Health* 18, 4 (2021), 2084.
- [75] Sang-il Lee, Hayoung Park, Jeong-Whun Kim, Hee Hwang, Eun-Young Cho, Yoon Kim, and Kyooseb Ha. 2012. Physicians’ perceptions and use of a health information exchange: A pilot program in South Korea. *Telemedicine and e-Health* 18, 8 (2012), 604–612.
- [76] Wen-Shan Jian, Shabbir Syed-Abdul, Sanjay P. Sood, Peisan Lee, Min-Huei Hsu, Cheng-Hsun Ho, Yu-Chuan Li, and Hsyien-Chia Wen. 2012. Factors influencing consumer adoption of USB-based Personal Health Records in Taiwan. *BMC Health Services Research* 12, 1 (2012), 1–8.
- [77] Rajesh R. Pai and Sreejith Alathur. 2020. Determinants of mobile health application awareness and use in India: An empirical analysis. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*. ACM, Athens Greece, 576–584.
- [78] Warrington Wen Qiang Hsu, Esther Wai Yin Chan, Zhang Jin Zhang, Zhi Xiu Lin, Zhao Xiang Bian, and Ian Chi Kei Wong. 2015. Chinese medicine students’ views on electronic prescribing: A survey in Hong Kong. *European Journal of Integrative Medicine* 7, 1 (2015), 47–54.
- [79] Josiah Dykstra, Rohan Mathur, and Alicia Spoor. 2020. Cybersecurity in medical private practice: Results of a survey in audiology. In *Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, Virtual, 169–176.
- [80] Rong Yin, Katherine Law, and David Neyens. 2021. Examining how internet users trust and access electronic health record patient portals: Survey study. *JMIR Human Factors* 8, 3 (2021), e28501.
- [81] Juhee Kwon and M. Eric Johnson. 2013. Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association* 20, 1 (2013), 44–51.
- [82] Jessica S. Ancker, Samantha Brenner, Joshua E. Richardson, Michael Silver, and Rainu Kaushal. 2015. Trends in public perceptions of electronic health records during early years of meaningful use. *The American Journal of Managed Care* 21, 8 (2015), e487.
- [83] Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. 2020. Why employees (still) click on phishing links: investigation in hospitals. *Journal of Medical Internet Research* 22, 1 (2020), e16775.
- [84] Ronald M. Salomon, Jennifer Urbano Blackford, S. Trent Rosenbloom, Sandra Seidel, Ellen Wright Clayton, David M. Dilts, and Stuart G. Finder. 2010. Openness of patients’ reporting with use of electronic records: Psychiatric clinicians’ views. *Journal of the American Medical Informatics Association* 17, 1 (2010), 54–60.
- [85] Kuang-Yi Wen, Gary Kreps, Fang Zhu, and Suzanne Miller. 2010. Consumers’ perceptions about and use of the internet for personal health records and health information exchange: analysis of the 2007 Health Information National Trends Survey. *Journal of Medical Internet Research* 12, 4 (2010), e1668.
- [86] Srinivas Emani, Cyrus K. Yamin, Ellen Peters, Andrew S. Karson, Stuart R. Lipsitz, Jonathan S. Wald, Deborah H. Williams, David W. Bates, et al. 2012. Patient perceptions of a personal health record: A test of the diffusion of innovation model. *Journal of Medical Internet Research* 14, 6 (2012), e2278.
- [87] Kyungsook Gartrell, A. M. Trinkoff, C. L. Storr, M. L. Wilson, and A. P. Gurses. 2015. Testing the electronic personal health record acceptance model by nurses for managing their own health. *Applied clinical informatics* 6, 02 (2015), 224–247.
- [88] Jolie N. Haun, Wendy Hathaway, Margeaux Chavez, Nicole Antinori, Brian Vetter, Brian K. Miller, Tracey L. Martin, Lisa Kendziora, Kim M. Nazi, and Christine Melillo. 2017. Clinical practice informs secure messaging benefits and best practices. *Applied Clinical Informatics* 8, 04 (2017), 1003–1011.
- [89] Michelle M. Mello, Van Lieou, and Steven N. Goodman. 2018. Clinical trial participants’ views of the risks and benefits of data sharing. *New England Journal of Medicine* 378, 23 (2018), 2202–2211.
- [90] Emily C. O’Brien, Ana Maria Rodriguez, Hye-Chung Kum, Laura E. Schanberg, Marcy Fitz-Randolph, Sean M. O’Brien, and Soko Setoguchi. 2019. Patient perspectives on the linkage of health data for research: Insights from an online patient community questionnaire. *International Journal of Medical Informatics* 127 (2019), 9–17.
- [91] Joshua E. Richardson and Jessica S. Ancker. 2015. Public perspectives of mobile phones’ effects on healthcare quality and medical data security and privacy: A 2-year nationwide survey. In *Proceedings of the AMA Annual Symposium*. American Medical Informatics Association, American Medical Informatics Association, San Francisco, CA, 1076.
- [92] Heathe Luz McNaughton, Ellen M. H. Mitchell, Emilia G. Hernandez, Karen Padilla, and Marta Maria Blandon. 2006. Patient privacy and conflicting legal and ethical obligations in El Salvador: Reporting of unlawful abortions. *American Journal of Public Health* 96, 11 (2006), 1927–1933.
- [93] O. S. Ayanlade, T. O. Oyeibisi, and B. A. Kolawole. 2019. Health information technology acceptance framework for diabetes management. *Heliyon* 5, 5 (2019), e01735.
- [94] Wendy Currie. 2016. Health organizations’ adoption and use of mobile technology in France, the USA and UK. *Procedia Computer Science* 98 (2016), 413–418.

- [95] Ilaria Montagni, Nicolas Roussel, Rodolphe Thiébaut, and Christophe Tzourio. 2021. Health care students' knowledge of and attitudes, beliefs, and practices toward the French COVID-19 app: Cross-sectional questionnaire study. *Journal of Medical Internet Research* 23, 3 (2021), e26399.
- [96] Maria Gabriella Melchiorre, Roberta Papa, Mieke Rijken, Ewout van Ginneken, Anneli Hujala, and Francesco Barbabella. 2018. eHealth in integrated care programs for people with multimorbidity in Europe: Insights from the ICARE4EU project. *Health Policy* 122, 1 (2018), 53–63.
- [97] Fiona Fylan and Beth Fylan. 2021. Co-creating social licence for sharing health and care data. *International Journal of Medical Informatics* 149 (2021), 104439.
- [98] Cecilia Pyper, Justin Amery, Marion Watson, and Claire Crook. 2004. Patients' experiences when accessing their on-line electronic patient records in primary care. *The British Journal of General Practice* 54, 498 (2004), 38.
- [99] Wiktoria Wilkowska and Martina Ziefle. 2012. Privacy and data security in E-health: Requirements from the user's perspective. *Health Informatics Journal* 18, 3 (2012), 191–201.
- [100] Renée R. Shield, Roberta E. Goldman, David A. Anthony, Nina Wang, Richard J. Doyle, and Jeffrey Borkan. 2010. Gradual electronic health record implementation: new insights on physician and patient adaptation. *The Annals of Family Medicine* 8, 4 (2010), 316–326.
- [101] Andre Maiorana, Wayne T. Steward, Kimberly A. Koester, Charles Pearson, Starley B. Shade, Deepalika Chakravarty, and Janet J. Myers. 2012. Trust, confidentiality, and the acceptability of sharing HIV-related patient data: Lessons learned from a mixed methods study about Health Information Exchanges. *Implementation Science* 7, 1 (2012), 1–14.
- [102] Ron Janes, Bruce Arroll, Stephen Buetow, Gregor Coster, Ross McCormick, and Iain Hague. 2005. Rural New Zealand health professionals' perceived barriers to greater use of the internet for learning. *Rural and Remote Health* 5, 4 (2005), 1–11.
- [103] Jared M. Bechtel, Erin Lepoire, Amy M. Bauer, Deborah J. Bowen, and John C. Fortney. 2021. Care manager perspectives on integrating an mHealth app system into clinical workflows: A mixed methods study. *General Hospital Psychiatry* 68 (2021), 38–45.
- [104] Desla Mancilla and Jackie Moczygemba. 2009. Exploring medical identity theft. *Perspectives in Health Information Management/AHIMA, American Health Information Management Association* 6, Fall (2009), 11.
- [105] Rezvan Rahimi and Batoul Khoundabi. 2021. Investigating the effective factors of using mHealth apps for monitoring COVID-19 symptoms and contact tracing: A survey among Iranian citizens. *International Journal of Medical Informatics* 155 (2021), 104571.
- [106] Rebecca Giguere, William Brown III, Ivan C. Balán, Curtis Dolezal, Titcha Ho, Alan Sheinfil, Mobolaji Ibitoye, Javier R. Lama, Ian McGowan, and Ross D. Cranston. 2018. 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 (2018), 393–400.
- [107] Grace Kenny, Yvonne O'Connor, Emmanuel Eze, Edmund Ndibuagu, and Ciara Heavin. 2017. A ground-up approach to mHealth in Nigeria: A study of primary healthcare workers' attitude to mHealth adoption. *Procedia Computer Science* 121 (2017), 809–816.
- [108] Hongru Yu, Haiyang Sun, Danyi Wu, and Tsung-Ting Kuo. 2019. Comparison of smart contract blockchains for healthcare applications. In *Proceedings of the AMIA Annual Symposium*. American Medical Informatics Association, American Medical Informatics Association, Washington, DC, 1266.
- [109] Abimbola Adanijo, Caoimhe McWilliams, Til Wykes, and Sagar Jilka. 2021. Investigating mental health service user opinions on clinical data sharing: Qualitative focus group study. *JMIR Mental Health* 8, 9 (2021), e30596.
- [110] Jordan P. Richardson, Cambray Smith, Susan Curtis, Sara Watson, Xuan Zhu, Barbara Barry, and Richard R. Sharp. 2021. Patient apprehensions about the use of artificial intelligence in healthcare. *NPJ Digital Medicine* 4, 1 (2021), 1–6.
- [111] Rebecca Schnall, Tracy Higgins, William Brown, Alex Carballo-Dieguez, and Suzanne Bakken. 2015. Trust, perceived risk, perceived ease of use and perceived usefulness as factors related to mHealth technology use. *Studies in Health Technology and Informatics* 216 (2015), 467.
- [112] Lynne Coventry, Dawn Branley-Bell, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Kalliopi Anastasopoulou. 2020. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *Proceedings of the International Conference on Human-Computer Interaction*. Springer, Springer, Copenhagen, Denmark, 105–122.
- [113] Marie-Camille Patoz, Diego Hidalgo-Mazzei, Olivier Blanc, Norma Verdolini, Isabella Pacchiarotti, Andrea Murru, Laurent Zukerwar, Eduard Vieta, Pierre-Michel Llorca, and Ludovic Samalin. 2021. Patient and physician perspectives of a smartphone application for depression: A qualitative study. *BMC Psychiatry* 21, 1 (2021), 1–12.
- [114] 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. 2019. Hopeful and concerned: Public input on building a trustworthy medical information commons. *Journal of Law, Medicine and Ethics* 47, 1 (2019), 70–87.
- [115] Ala Sarah Alaqra, Bridget Kane, and Simone Fischer-Hübner. 2021. Machine learning-based analysis of encrypted medical data in the cloud: Qualitative study of expert stakeholders' perspectives. *JMIR Human Factors* 8, 3 (2021), e21810.
- [116] Frank J. Manion, Robert J. Robbins, William A. Weems, and Rebecca S. Crowley. 2009. Security and privacy requirements for a multi-institutional cancer research data grid: An interview-based study. *BMC Medical Informatics and Decision Making* 9, 1 (2009), 1–40.
- [117] Aksel Tjora, Trung Tran, and Arild Faxvaag. 2005. Privacy vs. usability: A qualitative exploration of patients' experiences with secure Internet communication with their general practitioner. *Journal of Medical Internet Research* 7, 2 (2005), e368.

- [118] Joshua M. Pevnick, Maria Claver, Aram Dobalian, Steven M. Asch, Harris R. Stutman, Alan Tomines, and Paul Fu. 2012. Provider stakeholders' perceived benefit from a nascent health information exchange: A qualitative analysis. *Journal of Medical Systems* 36, 2 (2012), 601–613.
- [119] Leonie Heyworth, Justice Clark, Thomas B. Marcello, Allison M. Paquin, Max Stewart, Cliona Archambeault, and Steven R. Simon. 2013. Aligning medication reconciliation and secure messaging: Qualitative study of primary care providers' perspectives. *Journal of Medical Internet Research* 15, 12 (2013), e2793.
- [120] Alaa A. Abd-alrazaq, Noor Suleiman, Khaled Baagar, Noor Jandali, Dari Alhuwail, Ibrahim Abdalhakam, Saad Shahbal, Abdul-Badi Abou-Samra, and Mowafa Househ. 2021. Patients and healthcare workers experience with a mobile application for self-management of diabetes in Qatar: A qualitative study. *Computer Methods and Programs in Biomedicine Update* 1 (2021), 100002.
- [121] Aubrey Baker, Laurian Vega, Tom DeHart, and Steve Harrison. 2011. Healthcare and security: Understanding and evaluating the risks. In *Proceedings of the International Conference on Ergonomics and Health Aspects of Work with Computers*. Springer, Springer-Verlag, Orlando, FL, 99–108.
- [122] Indra Neil Sarkar and Justin Starren. 2002. Desiderata for personal electronic communication in clinical systems. *Journal of the American Medical Informatics Association* 9, 3 (2002), 209–216.
- [123] Donna M. Baldwin, Javán Quintela, Christine Duclos, Elizabeth W. Staton, and Wilson D. Pace. 2005. Patient preferences for notification of normal laboratory test results: A report from the ASIPS Collaborative. *BMC Family Practice* 6, 1 (2005), 1–7.
- [124] Sung J. Choi, M. Eric Johnson, and Jinhyung Lee. 2020. An event study of data breaches and hospital IT spending. *Health Policy and Technology* 9, 3 (2020), 372–378.
- [125] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS 2018)*. IEEE, Baltimore, MD, 197–216.
- [126] Mohiuddin Ahmed and Abu S. S. M. Barkat Ullah. 2017. False data injection attacks in healthcare. In *Proceedings of the Australasian Data Mining Conference*. Springer, Springer Singapore, Singapore, 192–202.
- [127] Amir Djenna and Diamel Eddine Saïdouni. 2018. Cyber attacks classification in IoT-based-healthcare infrastructure. In *Proceedings of the 2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, IEEE, Paris, France, 1–4.
- [128] Garrett A. Cavaliere, Reem Alfalasi, Gregory N. Jasani, Gregory R. Ciottone, and Benjamin J. Lawner. 2021. Terrorist attacks against healthcare facilities: A review. *Health Security* 19, 5 (2021), 546–550.
- [129] Mirza Mansoor Baig, Hamid GholamHosseini, and Martin J. Connolly. 2015. Mobile healthcare applications: System design review, critical issues and challenges. *Australasian Physical and Engineering Sciences in Medicine* 38, 1 (2015), 23–38.
- [130] Eugene Y. Chan and Najam U. Saqib. 2021. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior* 119 (2021), 106718.
- [131] Farkhondeh Hassandoust, Saeed Akhlaghpour, and Allen C. Johnston. 2021. 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 (2021), 463–471.
- [132] Elizabeth Stobert, David Barrera, Valérie Homier, and Daniel Kollek. 2020. Understanding cybersecurity practices in emergency departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu, Hawaii, 1–8.
- [133] Kundan Munjal and Rekha Bhatia. 2023. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex and Intelligent Systems* 9, 4 (2023), 3759–3786.
- [134] Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. 2021. HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks* 200 (2021), 108500.
- [135] Lanfang Sun, Xin Jiang, Huixia Ren, and Yi Guo. 2020. Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application. *IEEE Access* 8 (2020), 101079–101092.
- [136] P. Blessed Prince and S. P. Jeni Lovesum. 2020. Privacy enforced access control model for secured data handling in cloud-based pervasive health care system. *SN Computer Science* 1, 5 (2020), 239.
- [137] Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. 2019. Leveraging user-related internet of things for continuous authentication: A survey. *ACM Computing Surveys* 52, 3 (2019), 1–38.
- [138] Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2016. Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security* 7, 02 (2016), 49.
- [139] Michael Guckert, Kristina Milanovic, Jennifer Hannig, David Simon, Tamara Wettengl, Daniel Evers, Arnd Kleyer, Till Keller, and Jeremy Pitt. 2022. The disruption of trust in the digital transformation leading to health 4.0. *Frontiers in Digital Health* 4 (2022), 815573.
- [140] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zeschwitz. 2019. "If HTTPS were secure, i wouldn't need 2FA"-end user and administrator mental models of HTTPS. In *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, CA, 246–263.
- [141] Akhila Kunche, R. Kumar Puli, Sunitha Guniganti, and Danaiah Puli. 2011. Analysis and evaluation of training effectiveness. *Human Resource Management Research* 1, 1 (2011), 1–7.

- [142] Johan Lugnet, Åsa Ericson, Martin Lundgren, and Johan Wenngren. 2020. On the design of playful training material for information security awareness. In *Proceedings of the 6th International Conference on Design Creativity (ICDC 2020), 26-28 August, 2020, Oulu, Finland*. The Design Society, 239–246.
- [143] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. 2020. Riskio: A serious game for cyber security awareness and education. *Computers and Security* 95 (2020), 101827.
- [144] Adir Solomon, Michael Michaelshvili, Ron Bitton, Bracha Shapira, Lior Rokach, Rami Puzis, and Asaf Shabtai. 2022. Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems* 246 (2022), 108709.

Received 11 November 2022; revised 16 December 2023; accepted 18 January 2024