







# SOK: Evaluating Privacy and Security Vulnerabilities of Patients' Data in Healthcare

Faiza Tazi<sup>1</sup>, Josiah Dykstra<sup>2</sup>, Prashanth Rajivan<sup>3</sup>,  
and Sanchari Das<sup>1</sup>

<sup>1</sup> University of Denver, Denver, CO 80208, USA  
{Faiza.Tazi,sandas}@du.edu

<sup>2</sup> Designer Security, LLC., Severn, MD 21144, USA  
josiah@designersecurity.com

<sup>3</sup> University of Washington, Seattle, WA, USA  
prajivan@uw.edu

**Abstract.** Interactions in healthcare systems, by necessity, involve sharing sensitive information that must be protected. Thus, to understand the existing privacy and security research conducted in the context of healthcare organizations, we conducted a systematic literature review of  $N = 205$  papers that examine the security and privacy of patient data. We found that current research focuses heavily on the technological solutions, which are presented to benefit large-scale medical facilities such as hospitals, but generally ignore the unique security challenges of smaller private practices which might not have the resources to protect patient data. Additionally, only 18 (<9%) papers have conducted user studies to understand the patient and staff's risk perception of healthcare data. We conclude by identifying research gaps and provide potential solutions to enable robust data security for sensitive patient data.

**Keywords:** Literature review · Healthcare Data Privacy and Security

## 1 Introduction

With increased digitization in the healthcare sector, privacy risks and security concerns about data storage, access, and transfer among healthcare providers and patients have subsequently increased as well [55, 174]. Thus, information security has become an ongoing challenge in the healthcare sector with critical data breaches exposing sensitive records of millions of patients [10]. One such major data breach occurred in 2015 when a phishing scam exploited the credentials of five employees at *Anthem*, a health insurance organization, compromising the Personally Identifiable Information (PII) of 80 million individuals [194]. Data breaches in healthcare could occur for a variety of reasons, including a lack of employee awareness about data security, technological shortcomings, and the dearth of technological implementations [53]. Despite the proliferation of data security focused research in the community, the field lacks a comprehensive

synthesis and analysis of the body of healthcare privacy and security research especially from the user<sup>1</sup> perspective [14].

Towards this, we conducted a systematic literature review to provide a holistic overview and a basis for the research undertaken in this area which has been proven to be helpful in other domains [125]. We collected 2,903 research articles on data security and privacy preservation in healthcare organizations. Thereafter, we did a thematic analysis on a selected set of  $N = 205$  papers. From the  $N = 205$  papers, we further discuss insights from  $n1 = 97$  papers that focused on the technological implementation. Finally, we present an in-depth analysis of  $n2 = 18$  papers that are focused on the human (user) factors. We found that the majority of the security research done in healthcare focused on the technologies with a severe lack of focus on understanding and improving the human factor aspect. Furthermore, even among the work focused on technologies, we observed a gap in the research with applications to private practice healthcare organizations. The disparity is noteworthy.

Our contributions through this work are as follows:

- While other Systematizations of Knowledge (SoKs) have been published on specific technologies related to healthcare, ours is among the first to perform a systematic approach for structuring existing knowledge on security and privacy in healthcare organizations.
- In this SoK we make a holistic observation on security and privacy in healthcare and point out gaps that remain to protect patients' health data.
- To the best of our knowledge, our SoK is the first paper to focus on an overview of privacy and security research of patient data from a human perspective.

Our study concludes that the technological solutions are outpacing the foundational analysis of the ways the healthcare workforce is using and defending patient data today. Moreover, the 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 Method

Our systematic literature review includes a corpus of 205 papers published till February 14, 2021, collected from different digital libraries. The literature review comprised of six steps: (i) database search, (ii) title screening, (iii) abstract screening, (iv) full-text screening, (v) data extraction, and (vi) thematic analysis. *Inclusion Criteria*: Papers 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. We contacted publication venues and authors to obtain papers that were not available for public access, and obtained all the papers in our list.

---

<sup>1</sup> Throughout this work, we will refer to all individuals with access and responsibility for protecting healthcare data, including patients and healthcare workers, as *users*.

*Exclusion Criteria:* Papers were excluded if: (1) Papers 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.

Search	N= 2903	Database Search: ACM DL, Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed
Screening	N=352	Title Screening (Google Scholar)
	N=280	Duplicate Removal
	N=231	Quality Screening (Removal of work in progress)
Analysis	N = 205	Abstract and Full-text Screening
	n1 = 97	Technical Solutions
	n2= 18	User Studies

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

## 2.1 Database and Keyword-Based Search

We conducted our search by exploring seven digital technology and medical databases: ACM DL, Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. We specifically searched healthcare-focused journals in MEDLINE but were not able to find any relevant papers based on our topic of research, so we removed it from our database list. 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, a systematic analysis was conducted on the final collection of research articles. This procedure was adapted from prior literature reviews by Stowell et al. [185], Das et al. [51, 52], and other related works [123, 127, 139].

After the initial search to obtain the keywords we collected the papers through a keyword-based search as mentioned above, using the Publish or Perish<sup>2</sup> software for retrieving articles from Google Scholar. Thereafter, we

<sup>2</sup> <https://harzing.com/resources/publish-or-perish>.

explored individual digital libraries to collect papers relevant to this research. Boolean search strings were developed for searching databases including up to 88 AND/OR operators and 17 NOT operators across the following keyword terms: *Healthcare Data Security, Healthcare Data Breach, Healthcare Data Theft, Medical Data Theft, Medical Data Security, Medical Data Breach, Patient Data Security, Patient Data Theft, and Patient Data Breach*. Our initial database and keyword-based search resulted in a total of 2903 papers.

## 2.2 Title Screening: Google Scholar

We noticed that every other digital library except Google Scholar has a limited number of papers. Thus, we avoided title-based screening for these digital libraries. We conducted a title-based search with the above-mentioned keywords in Google Scholar. We also removed any patents or citation options from Google Scholar. In the title-based search we looked for the keywords in the title itself to emphasize on the relevance, resulting in a total of 352 papers.

## 2.3 Duplicate and Work-in-Progress Removal

In the next phase, we conducted the step of duplicate removal. We removed 72 duplicate articles, which left us with 280 papers. We also removed any papers which were a work in progress such as posters, extended abstracts, etc. We screened out self-identified work-in-progress papers or reviewed the paper to see if the papers were works-in-progress. Due to the varying nature of publication of these works we could not demarcate the papers based on their page numbers with an assumption that work-in-progress papers are short. However, we removed any papers which were shorter than four pages. After this procedure, we were left with a data set of 231 papers.

## 2.4 Abstract and Full-Text Screening

Each individual research paper was assessed to determine its relevance to the topic of our research by reviewing the abstract and full-text. To do this, two researchers trained in qualitative coding determined the relevance of the individual papers to the research by analyzing the abstract and full-text. If there were any discrepancies with determining the relevance to the research then a third researcher was introduced to resolve the issue. Thus, 26 papers were excluded in this phase. After this screening, there remained a total of  $N = 205$  papers on which we conducted our detailed thematic analysis [51].

## 2.5 Analysis

Our final set of data included a total of  $N = 205$  papers on which we conducted detailed analysis in two parts. First, a thematic analysis was conducted to evaluate specific aspects of the papers including technical applications and policies. Thereafter, a detailed analysis of the user studies was conducted to understand more about the user issues as per the goal of this work.

**Table 1.** Distribution of the number of papers based on the thematic analysis

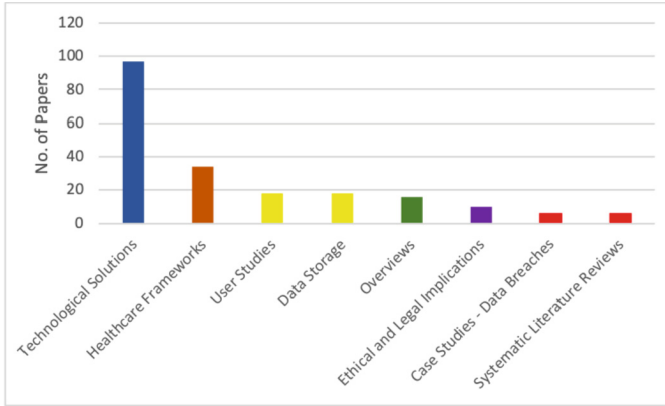
Themes	No. of papers
Technological solutions	97 (47.32%)
Healthcare frameworks	34 (16.58%)
User studies	18 (8.78%)
Data storage & Management	18 (8.78%)
Overviews	16 (7.80%)
Ethical and legal implications	10 (4.89%)
Case studies - Data breaches	6 (2.93%)
Systematic literature reviews	6 (2.93%)

**Thematic Analysis:** To perform a thematic analysis, we reviewed the abstract, methods, results, discussion, and conclusion of the 205 collected papers obtained from full-text screening. Two researchers evaluated this collection of papers by first reviewing 20 randomly selected papers to generate the codebook. The codebook consisted of 119 open codes which were themed into eight overarching themes including: technological solutions proposed, evaluation of current model with privacy frameworks, systematic literature reviews, evaluation of patient data focusing on the big data storage and management, ethical and legal implications of research, author notes and overview of the current healthcare practices to protect user data, case studies on particular incidents occurred as in data breaches, and finally the user studies.

Table 1 shows the distribution of the papers as per the categorization of all of the 205 papers. This can be further examined in Fig. 2. Any paper that included any form of user study, even if that was not the paper’s primary theme, was marked in the user study category. This was specified given the user-focused aspect of the paper. After conducting the first set of analysis, we performed another set of thematic analysis to categorize the papers which studied technological solutions to address healthcare privacy and security challenges. Given the large number of technical solution-focused papers, we have detailed them in Table 2 to explore more on what type of technical solutions were proposed by the prior works.

**User Study Analysis:** After the two phases of thematic analysis, we conducted a detailed user study analysis where we focused on the  $n2 = 18$  user studies. We extracted the quantitative and qualitative findings to assess what user and technical perspectives of the healthcare-focused research was conducted by the prior studies. We have provided details of both the technical solutions analyzed in this work and the user studies in the following section.

Out of the 18 user-focused studies, four were qualitative [1, 24, 48, 99], 12 were quantitative [23, 36, 43, 49, 69, 71, 80, 140, 143, 162, 170, 177], and two were mixed-methods studies [28, 133]. The quantitative studies included works which imple-



**Fig. 2.** A snapshot of the themes discussed throughout the analysis

mented nine survey-based studies [23, 49, 69, 71, 80, 143, 162, 170, 177], one cross-sectional studies [36], one in-lab simulation-based study [43], and one randomized control experiment [140]. For qualitative studies, they included three interview-based studies [1, 24, 48] and one field-based research [99]. In the qualitative study, Baker et al. also performed observation evaluations on their studied participants for the interview [24]. For mixed methods, there were two studies, where one study which had a combination of online survey and did content analysis [133], the second study did a semi-structured interview with 16 care managers at 12 health centers in three states participated [28].

### 3 Findings and Discussions

As described earlier, we first started with the thematic analysis of the collected papers where we found eight overarching themes. Thereafter, we detailed the technical solutions provided by the papers, and finally performed a detailed literature analysis on the small subset of user studies identified. In this section, we will first provide details of the thematic analysis and thereafter, we will provide details and evaluation of the user studies.

#### 3.1 Thematic Analysis

For each of the 205 papers, we collected details about the methods, results, analysis, discussion, and implications. Thereafter, we analyzed the data collected, and categorized them into eight themes as shown in Table 1. For this we particularly looked into the methods, results, and discussions of the mentioned papers. We then performed a detailed analysis on the technical solutions and the user studies, which will be discussed in the later subsections.

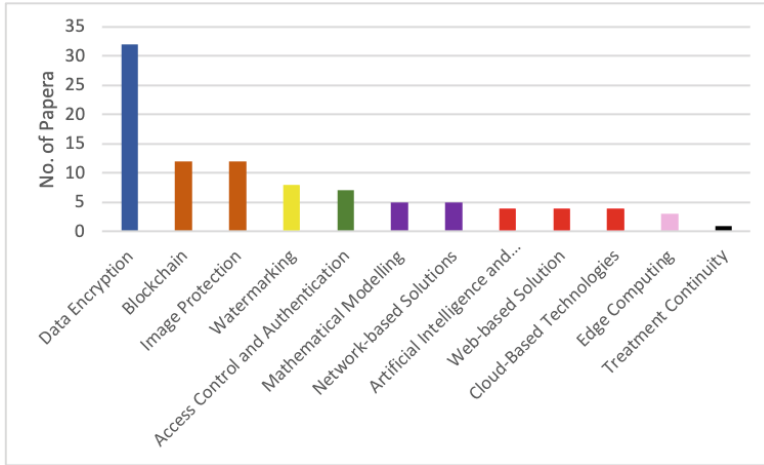
**Technical Solutions Discussed:** Nearly half of the collection,  $n1 = 97$  (47.32%) out of  $N = 205$  papers, focused on proposing a technology-based solution for the privacy and security issues of the healthcare sector. To understand further, we classified the technical solutions proposed by the authors. Table 2 as well as Fig. 3 show the distribution of the papers based on the several types of technological solutions proposed by the authors to enhance the privacy and security of the data transferred and accessed in the healthcare sector. Many of the papers use a combination of the technical solutions, for example using cryptography for authentication or using encryption to do image processing. However, here we used mutually exclusive codes to focus on the primary solution proposed by the paper after going through the full-text.

**Table 2.** Distribution of the papers providing technical solutions out of the  $n1 = 97$  papers which proposed privacy and security solutions of the healthcare organization

Themes	No. of papers
Data encryption	32 (32.99%)
Blockchain	12 (12.37%)
Image protection	12 (12.37%)
Watermarking	8 (8.25%)
Access control and Authentication	7 (7.22%)
Mathematical modelling	5 (5.15%)
Network-based solutions	5 (5.15%)
Artificial intelligence and Machine learning	4 (4.12%)
Web-based solution	4 (4.12%)
Cloud-based technologies	4 (4.12%)
Edge computing	3 (3.1%)
Treatment continuity	1 (1.03%)

*Data Encryption:* Out of the  $n1 = 97$  technology-focused papers, nearly half of the papers discussed the encryption techniques to protect the data. A total of 32.99% of the papers discussed how patient data can be encrypted and anonymized for robust security of health-related data [6, 16, 17, 25, 29–31, 42, 57, 86, 92, 96, 103, 120, 147, 153, 159, 161, 166, 167, 188, 189, 195, 197, 201, 209–211]. For example, Sudha and Ganesan while discussing the lack of security of Electronic Medical Records (EMR) propose a Pervasive Mobile Healthcare where multimedia medical record are protected using an Elliptical Curve Cryptography algorithm [186]. Gupta and Metha discuss the importance of transmission of medical data over unsecured networks, and propose a chaos-based encryption scheme to secure medical images [76].

*Blockchain:* Another important focus on the technological solution found in our collected sample was on blockchain technology [8, 13, 33, 38, 50, 72, 75, 112,



**Fig. 3.** A snapshot of different technology based solutions for healthcare data privacy and security

[149,154,155,181]. These papers explore the peer-to-peer network topology of the blockchain, which implements a distributed ledger technology focusing on the transparency of the network [141]. For example, Brunese et al. propose a blockchain-based technology aimed to protect 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 [38]. *Image Protection:* As discussed previously, there are papers which discussed how encryption and blockchain can be used to protect medical data in the form of images. However, we found 12 papers which explored the different technical implementations to specifically protect medical images [18,21,27,40,42,62,97,102,114,171,173,182]. For example, Kumar et al. propose embedding patient information into a medical image through data hiding to improve security and confidentiality for diffusion of medical information system [114]. Their proposal was interesting and effective as they not only discussed embedding the text into images, but also the importance of protecting these images.

*Watermarking:* A particular aspect of image protection was digital watermarking. There were eight papers which focused on the watermarking aspect of medical image protection [22,65,66,98,137,165,182,200]. Vidya and Padmaja focused on enhancing the security of Electronic Patient Record (EPR) data which enable tele-diagnosis. They propose watermarking by embedding EPR into the facial photograph of the patient and discussed implementing a Photoplethysmography signal from the forefinger tip of the patient for authentication which had a success rate of 98% against security breaches [200].

*Access Control and Authentication:* Seven papers focused on making the security protocols of the healthcare system robust by addressing the access control and authentication particularly [20,73,73,85,105,157,172]. Izza et al. focused on



Internet of Things-based E-healthcare and radio frequency identification (RFID) authentication scheme for Wireless Body Area Network (WBANs). In their protocol, which they mention to be effective against digital threats implements elliptic curve digital signature with message recovery [85].

*Mathematical Modeling:* We found that five of the collected papers utilized statistical and other mathematical models to provide solutions to the security threats of the healthcare organization [44, 121, 122, 124, 192]. Chaudhury et al. discusses the Supervisory Control And Data Acquisition (SCADA) systems used for medical data transfer and how Impulsive Statistical Fingerprinting (ISF) can be implemented to substantiate the conversion of sensitive health data through the ISF into a secure Health Level 7 (HL7) format [44].

*Network-based Solutions:* Five (5.15%) of the papers discussed network-based solutions to resolve the privacy and security complexities of healthcare systems [26, 88, 106, 206, 213]. For example, Wang et al. details the WBAN and introduces the key technologies and characteristics of wireless sensor networks emphasizing node localization. They emphasize the importance of network localization algorithms and performance evaluation indicators on wearable 3D node localization algorithms to protect healthcare data of the patients [206].

*AI and ML-based Solutions:* Out of  $n1 = 97$  papers we found that four (4.12%) papers discussed artificial intelligence and machine learning-based solution to address the privacy and security issues of the healthcare sector [45, 95, 156, 183]. PraveenKumar proposes health and temperature sensors to monitor the patient health data that gets transmitted to a microcontroller. The real time data is then monitored and analyzed using k-means clustering and can guide both patient and doctor knowledge [156].

*Web-based Solutions:* Web-based solutions were proposed in four papers in our collection, where any form of web-based technical solutions to improve privacy and security of the sensitive data of the patients was discussed [19, 117, 191, 207]. Tian et al. looked into clinical prognosis prediction models based on electronic health record data and 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 [191].

*Cloud-based Solutions:* Four out of 205 papers discussed cloud-based solutions to address the privacy and security issues of patient data protection [12, 58, 101, 134]. Khan et al. presents a secure cloud-based mobile healthcare framework using WBANs where the framework tries to secure the inter-sensor communication by multi-biometric-based key generation scheme [101].

*Edge Computing-based Solutions:* Several prior papers have discussed edge computing, but we found three papers which focused on edge-computing-based solutions [7, 9, 119]. Edge computing is a distributed, open IT architecture that features decentralised processing by the device itself or by a local computer or server, rather than being transmitted to a data center [175].

*Treatment Continuity:* An interesting paper by Zhang et al. [214] pointed out a scary aftermath of cybersecurity breaches, which is pausing or preventing continuous treatment of patients suffering from critical ailments. Their proposed solution to address this focuses on automatic retrieval of essential information from the clinical radiation oncology information systems for each under-treatment patient periodically and providing backup through secondary data servers in the event of an attack to one of the servers [214].

**Healthcare Frameworks:** Of the 205 papers collected, 34 (16.58%) papers studied or introduced new healthcare data management frameworks. A paper was considered under the theme of healthcare frameworks if the main subject of its study is a security, privacy, or design frameworks [5, 11, 15, 35, 37, 39, 60, 67, 70, 83, 84, 90, 110, 113, 115, 116, 118, 126, 128, 132, 135, 145, 150, 152, 160, 164, 178, 180, 198, 208]. These papers particularly describe methods to design a secure and private technology for healthcare data usage. One such paper “A Security Framework for Mobile Health Applications” introduced a security framework for healthcare mobile applications, taking usability and security into consideration [190]. Ibrahim et al. introduced a framework for securely sharing electronic health records over the cloud between different healthcare providers. This framework ensures the confidentiality, integrity, authenticity, availability, and auditability of the electronic health records [82].

**Data Storage and Management:** Papers were classified as data storage and management if the research done was related to healthcare data access, manipulation, or the different technologies allowing for medical data storage. We found 18 (8.78%) such papers in our corpus [32, 54, 68, 74, 77, 81, 94, 107–109, 129, 138, 151, 163, 168, 179, 202, 205]. In particular, Duque et al. introduce a distributed data management architecture with a focus on the healthcare data security and high performance requirements [54]. On the other hand, Petković was concerned about the reliability of data transmitted through remote patient monitoring systems, since the data is collected by patients with no medical supervision [151]. Petrović addresses this issue by proposing several approaches that minimize the risks and ensure high information reliability.

**Overviews:** Overview papers include works which consolidate the prior work on healthcare privacy and security by adding details of the current state of privacy and security in the organizations and also adding details of the new technologies implemented. Of the 205 papers, 16 papers (7.80%) discuss or review the healthcare privacy and security domain [2–4, 41, 59, 100, 100, 130, 142, 144, 148, 158, 187, 196, 204]. Of these, Paksuniemi et al. gives an overview of the wireless technologies devices and reveal the importance of implementing security measures in these technologies to enable secure patient monitoring [144]. Moreover, Wang provides an overview of the security threats imposed by smart devices which monitor the patients through internet-connected technologies. Wang details two

primary security related issues for Internet-based tele-medicine systems that need to be addressed: (1) medical data protection needs; and (2) system design issues [204].

**Ethical and Legal Implications:** Of the 205 papers, ten (4.89%) papers studied the ethical and legal ramifications of data leaks occurring due to healthcare data breaches [63, 72, 78, 79, 91, 104, 131, 169, 193, 199]. These papers particularly explore violations in U.S. healthcare standards, including the Health Information Technology for Economic and Clinical Health (HITECH) Act [79] which proposes the meaningful use of interoperable electronic health records throughout the U.S. healthcare delivery system as a critical national goal. Hollis also discusses how beyond medical data security, healthcare staff are ethically required to anonymize the data so other staff are unable to uniquely identify a patient through their stored data [78].

**Case Studies and Data Breaches:** Case studies and data breaches both document real-world outcomes including common violations of security and privacy. Both are insightful to illuminate contemporary issues and research should seek to help develop proactive defenses that decrease the prevalence and impact of incidents and data breaches. We found that six (2.93%) of the 205 corpus papers were case studies and data breaches, classified as such when authors studied a particular organization, data protection practices, or particular incidents of data breaches. Some of these case studies chose different countries for their analysis [34, 46, 61, 136, 176, 212]. The organizations which were studied spanned global geography including India [176], United States [46], Saudi Arabia [34], and Morocco [136].

Yesmin and Carter created an evaluation framework for automated privacy auditing and found that 98.09% of 55,000 accesses of protected health information by staff in a hospital were identified as appropriate and the tool was unable to identify the remaining 1.91% of accesses [212]. Choi et al.'s work estimated changes in health information technology investments by tracking spending by U.S. hospitals between 2012 and 2016. Their results found that health information technology spending increased by 26.0% in one year after a breach [46]. These studies have been critical to understanding the real world but do not mention the stakeholders who were responsible or whose data were breached and how that may impact patients' lives.

**Systematic Literature Reviews:** Of the 205 papers analyzed, six (2.93%) were systematic literature reviews [47, 87, 89, 93, 146, 203]. These studies gave an overview of the current standards and practices followed in the healthcare sectors while mentioning the importance of the focus on the healthcare privacy and security. However, these studies did not focus or explore the user perspective. For example, Walker et al. implemented a mixed-method systematic review by analyzing about 300,000 papers 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 insiders attack [203].

### 3.2 Analysis of User Studies

In addition to our analysis of the technical solutions proposed in the collection, we performed a detailed analysis of the user studies ( $n = 18$ ). Our goal was to understand and assess the studies which evaluated user perception towards the privacy and security of their healthcare-related data. We performed a thorough analysis of the user studies and analyzed certain aspects of the study such as type of study conducted, study populations, duration, and medical settings.

**Table 3.** % of and number of studies in settings with various population densities along with details about the user study durations.

	Qual studies (n = 4)	Quant studies (n = 12)	Mixed- Methods (n = 2)
<b>Population</b>			
Urban	25% (1)	41.67% (5)	0% (0)
Suburban	0% (0)	0% (0)	0% (0)
Rural	25% (1)	0% (0)	0% (0)
Mixed	0% (0)	8.33% (1)	50% (1)
Other	0% (0)	0% (0)	0% (0)
Not reported	50% (2)	50% (6)	50% (1)
<b>Study population setting</b>			
Healthcare Providers	75% (3)	33.33% (4)	100% (2)
Healthcare Students	0% (0)	25% (3)	0% (0)
Patients	0% (0)	8.33% (1)	0% (0)
Mixed	25% (1)	16.66% (2)	0% (0)
General Population	0% (0)	16.66% (2)	0% (0)
<b>Study location</b>			
USA	25% (1)	16.66% (2)	50% (1)
Europe	25% (1)	25% (3)	50% (1)
Europe and USA	0% (0)	8.33% (1)	0% (0)
Asia	0% (0)	25% (3)	0% (0)
Middle East	25% (1)	8.33% (1)	0% (0)
Nigeria	25% (1)	8.33% (1)	0% (0)
Turkey	0% (0)	8.33% (1)	0% (0)

**Study Method:** Of the 18 user studies in our corpus, 66.66% (12) were quantitative studies. From the quantitative perspective, 50% (9) were surveys [23, 49, 69, 71, 80, 143, 162, 170, 177], 5.56% (1) quantitative descriptive study [36], 5.56% (1) simulation-based study for a quantitative sample [43], 5.56% (1) randomized controlled trials [140]. Of other studies, 11.1% (2) were mixed-methods survey [28, 133] with open-ended questions with a smaller population sample, 5.56% (1) field study [99], and 16.66% (3) qualitative interview-based studies [1, 24, 48]. Among the 18 user studies, only one assessed a proposed technological intervention. This evaluation involved the efficiency and convenience of a mobile app for managing diabetes [1]. Participants noted that one advantage of it was compliance with hospital regulations for patient data security.

**Study Duration:** For the majority of the studies, the time taken for the completion of the study primarily occurred in a single session (Table 3) [23, 49, 69, 71, 133, 143, 170, 177]. However, an evaluation of a diabetes management app occurred over 12 weeks [1], the randomized controlled trial of telehealth occurred over a 12 month period [140]. Also, a survey of public perception mobile phones' effect on healthcare was repeated in 2013 and 2014 [162], and a field study in Nigeria was conducted over four weeks [99]. Such longitudinal studies are particularly important to understand users' privacy and security perspective and how user perspectives can change (or do not change) over time.

**Population Distribution:** As shown in Table 3, many of the 18 papers did not report population distribution of the participants (44.44%, 8) [23, 28, 49, 69, 99, 143, 177]. Most of the remainder studies were conducted in urban settings (37.5%, 6) [1, 36, 43, 80, 140, 170], except one (5.56%) which was conducted in a rural setting [24]. No papers reported on suburban population settings.

**Study Population Setting:** Of nine of the 18 user-focused papers which studied healthcare providers [24, 28, 48, 49, 69, 71, 99, 133, 177], only one studied the patients exclusively [170]. Three papers studied a mixed population of patients and healthcare providers [1, 23, 140]. Mixed method studies focused only on healthcare providers; similarly, 75% of qualitative studies were focused on healthcare providers.

**Study Geographical Location:** Out of the 18 studies, four were conducted in the USA [24, 28, 140, 162] and five in the European Union [48, 69, 71, 133, 177], and one was conducted in both Europe and USA [49]. One paper that conducted their study with participants in Europe included 30 countries [177] and one included 24 European countries [133]. Only one study was conducted in Turkey [36], two in Africa (both in Nigeria) [23, 99], and two in the Middle East [1, 170]. Three quantitative studies were conducted in Asia specifically India, Malaysia, and Hong Kong [43, 80, 143].

**Table 4.** % and Number of studies conducted in various healthcare facilities along with the number of study participants for different user studies.

	Qual studies (n = 4)	Quant studies (n = 12)	Mixed- Methods (n = 2)
<b>Studied medical facilities</b>			
Home	0% (0)	16.67% (2)	0% (0)
Hospital	25% (1)	25% (3)	0% (0)
Private practice	25% (1)	0% (0)	0% (0)
Mixed	0% (0)	16.67% (2)	0% (0)
Other medical	50% (2)	41.67% (5)	50% (1)
Not reported	0% (0)	0% (0)	50% (1)
<b>Num participants</b>			
>0, ≤100	75% (3)	0% (0)	50% (1)
>100, ≤500	0% (0)	50% (6)	50% (1)
>500, ≤1000	0% (0)	14.67% (5)	0% (0)
>1000, ≤5000	0% (0)	8.33% (1)	0% (0)
>5000	0% (0)	0% (0)	0% (0)
Not reported	25% (1)	0% (0)	0% (0)

**Study Context:** Two qualitative studies were conducted in medical settings other than hospitals and private practice [1,99]; one was conducted in private practices [24] and one in three different hospitals [48]. (Table 4). Quantitative studies reported settings including hospitals [69,71,177], medical settings not including hospitals and private practice such as medical schools [36,43,49,80,143], patients' home environments [162,170], and mixed settings [23,140]. No papers focused on private practice settings. This is again interesting, as privacy and security of medical data is critical irrespective of the setting. Thus, studies focusing on more diverse medical settings are critical.

**Number of Participants:** One of the 4 qualitative studies did not report the sample size. The most participants reported in one study is 50 participants, the other two studies reported the same number of participants, 14. All the quantitative studies and the mixed method studies reported the sample size. A total of 94 participants were in qualitative studies, 5,856 (Median=429, IQR=581, Range=50–1242) were in quantitative studies, and 117 (Median=58.5, IQR=42.5, Range=16–101) in mixed studies.

## 4 Implications

We acknowledge the contribution of these previous works towards enhancing the privacy and security of sensitive patient data. However, we note that more

research is needed to fully understand the challenges to healthcare security and privacy.

#### 4.1 Holistic Security Approach

When security or privacy are a secondary goal of the users, research is needed to understand the motivations behind the circumvention of controls. From our analysis of the user studies, we have identified three major themes pertaining to the human factors of information security in healthcare, namely: inconsistent access controls, non-compliant and insecure communication modes, and disruptive update and backup policies. The majority of the past security research involving people in healthcare has focused on understanding how providers may circumvent authentication [184], including the discovery that providers often share login credentials with each other due to inconsistencies in access control policies [24, 48].

Access controls and privileges in healthcare are often designed without considering the individual provider's needs or the multitude of tasks conducted by them on a day-to-day basis. Rather, it is often designed in a tiered manner where senior doctors have the most privileges and junior doctors and nurses are assigned limited privileges [24, 48, 69]. Therefore whenever a provider (e.g., nurse or junior doctor) needs immediate access to a certain system or patient record for providing critical care, but don't have the necessary privileges, credentials are shared, usually by the senior doctors in these settings. This type of credential sharing also occurs when someone needs access at a critical time but has not completed the necessary training [47]. In addition to this, past research also discusses other general, known issues associated with password usage such as using insecure passwords, task interruptions, disabling authentication or keeping machines unlocked for a long periods of time. Access control cards are used to counter these password usage issues, but still do not address the security circumvention issues discussed earlier [177].

The other dominant theme involved secure communication between providers and patients, or lack thereof. Few papers noted that providers often used non-HIPAA compliant messaging software to share test results with the patients and also with each other [1, 48]. For example, providers have been known to share images of scan reports with patients using WhatsApp, a popular messaging platform from Facebook. Providers may be placing inappropriate trust on these messaging platforms based on the end-to-end encryption claims made by these platforms. More research is necessary to understand the challenges involving the use of recognized, HIPAA compliant message systems (e.g., American Messaging System or AS) for communicating securely between providers and between providers and patients.

The final theme that emerged from our analysis was regarding the issue of applying security updates and automatic backups. Providers report updates and backups appearing at inappropriate times such as while engaging with patients [48]. More research is necessary to determine the timing of updates that are reasonably quick and non-disruptive to the workflow of the providers.

Unsurprisingly, technologies including encryption, blockchain, cloud, and access controls were popular topics in the research literature. While technology represents an important area for future opportunities and threats in healthcare, they remain distant and disconnected from real-world needs today. Their overrepresentation in the literature, therefore, overshadows the analysis of security and privacy practices today.

The rollout of any new technology in healthcare is slow given strict legal and compliance constraints. Despite these new technologies, other technical solutions were notably missing that may hold promise for healthcare security and privacy. For example, continuous authentication may aid healthcare workers by using biometrics or hardware tokens to lock and unlock computers when an authorized user is in physical proximity. The user studies of security circumvention suggest that automated security features may be helpful, building on the effectiveness of features such as automated software updates. Additionally, despite the popularity of machine learning solutions in various fields, we were surprised that these solutions were not prominent in our healthcare corpus.

## 4.2 Focus on Private Practice Healthcare

The studies we analyzed focused heavily on hospitals and other large medical settings despite the fact that those represent a narrow view of all healthcare workplace settings. Hospitals are atypical because they are among the most well-resourced settings for controlling, implementing, and enforcing security and privacy controls. Those resources enable higher than average investment in security and privacy solutions, technical support, and organizational security culture. The problems that manifest in hospitals, and solutions for them, should not be assumed to generalize to other medical settings.

The literature appears to emphasize that improving health is the primary objective in healthcare, with security and privacy among secondary goals. A small businesses may have slimmer margins to apply to those non-primary goals. They need help to prioritize spending and implementation of privacy and security controls and the research community should prioritize the most impactful needs first. In a study of private practice audiology clinics, Dykstra et al. found that expertise, time, and money were reported as the primary limitations of better cybersecurity [56]. While these limitations are not unique to healthcare, they must be more explicitly acknowledged when proposing new security and privacy mitigation measures. For example, one might imagine that a doctor in a single-provider clinic may circumvent a compliant telehealth solution and revert to a non-compliant personal device given a hardware failure in the practice. Thus, a focus on studies reviewing such nuances will be critical especially for private practice and other resource-constrained healthcare organizations.

## 4.3 Studies in Rural Setting and Developing Nations

Along these lines, we observed scarce security and privacy research related to rural settings and developing nations. The resource limitations of the settings



demand a dedicated study of the population and appropriate technological mitigation techniques. The healthcare sector and research communities alike require the insights of economics. None of the papers in our survey offered a robust analysis of the probability of various vulnerabilities that would aid resource-limited organizations in prioritizing solutions. Economic models, such as the Gordon-Loeb model, may be effective in suggesting investment strategies [64]. Economics research may also wish to explore the costs and benefits of cybersecurity policy decisions in medical settings, insights about attacker motivations, and oppositional human factors to disrupt attacker cognition and decision making.

#### 4.4 Understanding the Patient's Perspective

Among the user studies we analyzed, the majority have focused on understanding the security behaviors of healthcare workers. However, patients' perspectives appears to be largely overlooked. Security and privacy requirements should be informed and driven primarily from the desires of patients about their own data. Patients as voting citizens influence healthcare laws and regulations in their choice of elected officials. Patients are also the most directly impacted by security breaches. More research is necessary to understand the gaps in patients' understanding about the implications of a security breach to their personal data. Research is also necessary to understand how much (or how little) trust patients place in their healthcare organizations in protecting their personal data [111].

## 5 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 important 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. Further, past research has drawn heavily from surveys so in-situ data would provide further grounding and accuracy.

## 6 Conclusion

As the healthcare sector is increasingly digitized, privacy risks and security concerns about data storage, access, and transfer have greatly increased. However, the question remains about how the research community is addressing these concerns from the technical and user perspective. To this aid, we conducted a detailed systematic literature review after collecting 2,903 papers and thematically analyzing  $N = 205$  of them. These peer-reviewed research articles were published and available over seven digital spaces: ACM DL, Google Scholar,

SSRN, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. We examined the security and privacy of patient data in healthcare organizations as studied by prior literature. We found that current research focuses primarily on data encryption and frameworks while understudying the user risk perceptiveness of privacy and security. Along the socio-technical component of healthcare privacy and security, it was concerning to note that < 9% of the papers 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 primarily on larger 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.

**Acknowledgments.** We would like to 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 in this research and Alisa Zezulak for helping with the proofreading of this paper. Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views of the University of Denver, the University of Washington, and the Designer Security.

## References

1. Abd-alrazaq, A.A., et al.: Patients and healthcare workers experience with a mobile application for self-management of diabetes in Qatar: a qualitative study. *Comput. Methods Program. Biomed. Update* **1**, 100002 (2021)
2. Abouelmehdi, K., Beni-Hessane, A., Khaloufi, H.: Big healthcare data: preserving security and privacy. *J. Big Data* **5**(1), 1–18 (2018). <https://doi.org/10.1186/s40537-017-0110-7>
3. Abouelmehdi, K., Beni-Hessane, A., Khaloufi, H., Saadi, M.: Big data security and privacy in healthcare: a review. *Procedia Comput. Sci.* **113**, 73–80 (2017)
4. Abraham, C., Chatterjee, D., Sims, R.R.: Muddling through cybersecurity: insights from the us healthcare industry. *Bus. Horiz.* **62**(4), 539–548 (2019)
5. Acharya, S., Susai, G., Pillai, M.: Patient portals: Anytime, anywhere, pp. 779–781 (2015)
6. Aiswarya, R., Divya, R., Sangeetha, D., Vaidehi, V.: Harnessing healthcare data security in cloud, pp. 482–488 (2013)
7. Al Hamid, H.A., Rahman, S.M.M., Hossain, M.S., Almogren, A., Alamri, A.: A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access* **5**, 22313–22328 (2017)
8. Al-Karaki, J.N., Gawanmeh, A., Ayache, M., Mashaleh, A.: Dass-care: a decentralized, accessible, scalable, and secure healthcare framework using blockchain, pp. 330–335 (2019). <https://doi.org/10.1109/IWCMC.2019.8766714>
9. Alam, M.G.R., Munir, M.S., Uddin, M.Z., Alam, M.S., Dang, T.N., Hong, C.S.: Edge-of-things computing framework for cost-effective provisioning of healthcare data. *J. Parallel Distrib. Comput.* **123**, 54–60 (2019)

10. Albarrak, A.I.: Information security behavior among nurses in an academic hospital. *Health Med.* **6**(7), 2349–2354 (2012)
11. Alboaie, S., Nita, L., Stefanescu, C.: Executable choreographies for medical systems integration and data leaks prevention, pp. 1–4 (2015). <https://doi.org/10.1109/EHB.2015.7391612>
12. Almeahadi, T., Alshehri, S., Tahir, S.: A secure fog-cloud based architecture for MIoT, pp. 1–6 (2019). <https://doi.org/10.1109/CAIS.2019.8769524>
13. Alshalali, T., M'Bale, K., Josyula, D.: Security and privacy of electronic health records sharing using hyperledger fabric, pp. 760–763 (2018). <https://doi.org/10.1109/CSCI46756.2018.00152>
14. Altuntaş, G., Semerciöz, F., Eregez, H.: Linking strategic and market orientations to organizational performance: the role of innovation in private healthcare organizations. *Procedia-Soc. Behav. Sci.* **99**, 413–419 (2013)
15. Alyami, H., Feng, J.L., Hilal, A., Basir, O.: On-demand key distribution for body area networks for emergency case (2014). <https://doi.org/10.1145/2642668.2642684>
16. Anghelescu, P.: Encryption of multimedia medical content using programmable cellular automata, pp. 11–16 (2012)
17. Anghelescu, P., Ionita, S., Sofron, E.: Block encryption using hybrid additive cellular automata, pp. 132–137 (2007)
18. Arumugham, S., Rajagopalan, S., Rayappan, J.B.B., Amirtharajan, R.: Networked medical data sharing on secure medium-a web publishing mode for DICOM viewer with three layer authentication. *J. Biomed. Inf.* **86**, 90–105 (2018)
19. Asija, R., Nallusamy, R.: Data model to enhance the security and privacy of healthcare data, pp. 237–244 (2014). <https://doi.org/10.1109/GHTC-SAS.2014.6967590>
20. Aski, V., Dhaka, V.S., Kumar, S., Parashar, A., Ladagi, A.: A multi-factor access control and ownership transfer framework for future generation healthcare systems, pp. 93–98 (2020). <https://doi.org/10.1109/PDGC50313.2020.9315840>
21. Ayad, H., Khalil, M.: A semi-blind information hiding technique using DWT-SVD and QAM-16 for medical images, pp. 1–7 (2017)
22. Ayad, H., Khalil, M.: A semi-blind information hiding technique using DWT-SVD and QAM-16 for medical images (2017). <https://doi.org/10.1145/3090354.3090433>
23. Ayanlade, O., Oyebisi, T., Kolawole, B.: Health information technology acceptance framework for diabetes management. *Heliyon* **5**(5), e01735 (2019)
24. Baker, A., Vega, L., DeHart, T., Harrison, S.: Healthcare and security: understanding and evaluating the risks, pp. 99–108 (2011)
25. Balamurugan, G., Joseph, K.S., Arulalan, V.: An iris based reversible watermarking system for the security of teleradiology, pp. 1–6 (2016)
26. Bao, S.D., Chen, M., Yang, G.Z.: A method of signal scrambling to secure data storage for healthcare applications. *IEEE J. Biomed. Health Inf.* **21**(6), 1487–1494 (2017). <https://doi.org/10.1109/JBHI.2017.2679979>
27. Basavegowda, R., Seenappa, S.: Electronic medical report security using visual secret sharing scheme, pp. 78–83 (2013)
28. Bechtel, J.M., Lepoire, E., Bauer, A.M., Bowen, D.J., Fortney, J.C.: Care manager perspectives on integrating an mhealth app system into clinical workflows: a mixed methods study. *Gener. Hospital Psychiatry* **68**, 38–45 (2021)
29. Beshar, K.M., Subah, Z., Ali, M.Z.: IoT sensor initiated healthcare data security. *IEEE Sens. J.* **21**(10), 11977–11982 (2020)

30. Bharghavi, G., Kumar, P.S., Geetha, K., Sasikala Devi, N.: An implementation of slice algorithm to enforce security for medical images using DNA approach, pp. 0984–0988 (2018). <https://doi.org/10.1109/ICCSP.2018.8524413>
31. Bharghavi, G., Kumar, P.S., Geetha, K., Devi, N.S.: An implementation of slice algorithm to enforce security for medical images using DNA approach, pp. 0984–0988 (2018)
32. Bhola, J., Soni, S., Cheema, G.K.: Recent trends for security applications in wireless sensor networks—a technical review, pp. 707–712 (2019)
33. Bhuiyan, M.Z.A., Zaman, A., Wang, T., Wang, G., Tao, H., Hassan, M.M.: Blockchain and big data to transform the healthcare, pp. 62–68 (2018)
34. Binobaid, S., Fan, I.S., Almeziny, M.: Investigation interoperability problems in pharmacy automation: a case study in Saudi Arabia. *Procedia Comput. Sci.* **100**, 329–338 (2016)
35. Boddy, A., Hurst, W., Mackay, M., El Rhalibi, A.: A study into detecting anomalous behaviours within healthcare infrastructures, pp. 111–117 (2016)
36. Bodur, G., Gumus, S., Gursoy, N.G.: Perceptions of Turkish health professional students toward the effects of the internet of things (IOT) technology in the future. *Nurse Educ. Today* **79**, 98–104 (2019)
37. Branley-Bell, D., et al.: Your hospital needs you: eliciting positive cybersecurity behaviours from healthcare staff using the aide approach. *Ann. Disaster Risk Sci.* **3**(1), 1–16 (2020)
38. Brunese, L., Mercaldo, F., Reginelli, A., Santone, A.: A blockchain based proposal for protecting healthcare systems through formal methods. *Procedia Comput. Sci.* **159**, 1787–1794 (2019)
39. Brunese, L., Mercaldo, F., Reginelli, A., Santone, A.: Formal modeling for magnetic resonance images tamper mitigation. *Procedia Comput. Sci.* **159**, 1803–1810 (2019)
40. Brunese, L., Mercaldo, F., Reginelli, A., Santone, A.: Radiomic features for medical images tamper detection by equivalence checking. *Procedia Comput. Sci.* **159**, 1795–1802 (2019)
41. Burke, W., Oseni, T., Jolfaei, A., Gondal, I.: Cybersecurity indexes for ehealth, pp. 1–8 (2019)
42. Cao, F., Huang, H.K., Zhou, X.: Medical image security in a HIPAA mandated PACS environment. *Computer. Med. Imaging Graph.* **27**(2–3), 185–196 (2003)
43. Chan, K.G., Pawi, S., Ong, M.F., Kowitlawakul, Y., Goy, S.C.: Simulated electronic health documentation: a cross-sectional exploration of factors influencing nursing students' intention to use. *Nurse Educ. Pract.* **48**, 102864 (2020)
44. Chaudhry, J., Qidwai, U., Miraz, M.H.: Securing big data from eavesdropping attacks in scada/ics network data streams through impulsive statistical fingerprinting, pp. 77–89 (2019)
45. Chen, Y., Chen, W.: Finger ECG-based authentication for healthcare data security using artificial neural network, pp. 1–6 (2017)
46. Choi, S.J., Johnson, M.E., Lee, J.: An event study of data breaches and hospital IT spending. *Health Policy Technol.* **9**(3), 372–378 (2020)
47. Coventry, L., Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas* **113**, 48–52 (2018)
48. Coventry, L., et al.: Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour, pp. 105–122 (2020)
49. Currie, W.: Health organizations' adoption and use of mobile technology in France, the USA and UK. *Procedia Comput. Sci.* **98**, 413–418 (2016)

50. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **39**, 283–297 (2018)
51. Das, S., Kim, A., Tingle, Z., Nippert-Eng, C.: All about phishing: Exploring user research through a systematic literature review. arXiv preprint [arXiv:1908.05897](https://arxiv.org/abs/1908.05897) (2019)
52. Das, S., Wang, B., Tingle, Z., Camp, L.J.: Evaluating user perception of multi-factor authentication: a systematic review. In: *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)* (2019)
53. Demjaha, A., Caulfield, T., Sasse, M.A., Pym, D.: 2 fast 2 secure: a case study of post-breach security changes, pp. 192–201 (2019)
54. Duque, H., Montagnat, J., Pierson, J.M., Brunie, L., Magnin, I.: Dm2: a distributed medical data manager for grids, pp. 138–147 (2003)
55. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **19**(2), 326 (2019)
56. Dykstra, J., Mathur, R., Spoor, A.: Cybersecurity in medical private practice: results of a survey in audiology, pp. 169–176 (2020). <https://doi.org/10.1109/CIC50333.2020.00029>
57. El Bouchti, A., Bahsani, S., Nahhal, T.: Encryption as a service for data healthcare cloud security, pp. 48–54 (2016)
58. Elmogazy, H., Bamasak, O.: Towards healthcare data security in cloud computing, pp. 363–368 (2013)
59. Esposito, C., Castiglione, A.: Cloud-based management of healthcare data: security and privacy concerns and a promising solution
60. Essa, Y.M., Hemdan, E.E.D., El-Mahalawy, A., Attiya, G., El-Sayed, A.: IFHDS: intelligent framework for securing healthcare bigdata. *J. Med. Syst.* **43**(5), 1–13 (2019)
61. Garner, S.A., Kim, J.: The privacy risks of direct-to-consumer genetic testing: a case study of 23 and Me and ancestry. *Wash. UL Rev.* **96**, 1219 (2018)
62. Geetha, R., Geetha, S.: Efficient high capacity technique to embed EPR information and to detect tampering in medical images. *J. Med. Eng. Technol.* **44**(2), 55–68 (2020)
63. Georgiou, D., Lambrinouidakis, C.: Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR). *Information* **11**(12), 586 (2020)
64. Gordon, L.A., Loeb, M.P., Zhou, L., et al.: Investing in cybersecurity: insights from the Gordon-Loeb model. *J. Inf. Secur.* **7**(02), 49 (2016)
65. Goudar, V., Potkonjak, M.: Addressing biosignal data sharing security issues with robust watermarking, pp. 618–626 (2014). <https://doi.org/10.1109/SAHCN.2014.6990402>
66. Goudar, V., Potkonjak, M.: On admitting sensor fault tolerance while achieving secure biosignal data sharing, pp. 266–275 (2014). <https://doi.org/10.1109/ICHI.2014.44>
67. Goudar, V., Potkonjak, M.: A robust watermarking technique for secure sharing of basn generated medical data, pp. 162–170 (2014)
68. Gritzalis, D.: A baseline security policy for distributed healthcare information systems. *Comput. Secur.* **16**(8), 709–719 (1997)
69. Gritzalis, D., Katsikas, S., Keklikoglou, J., Tomaras, A.: Determining access rights for medical information systems. *Comput. Secur.* **11**(2), 149–161 (1992)

70. Gritzalis, D., Lambrinouidakis, C.: A security architecture for interconnecting health information systems. *Int. J. Med. Inf.* **73**(3), 305–309 (2004)
71. Gritzalis, D., Tomaras, A., Katsikas, S., Keklikoglou, J.: Data security in medical information systems: the Greek case. *Comput. Secur.* **10**(2), 141–159 (1991)
72. Gross, M.S., Miller Jr, R.C.: Ethical implementation of the learning healthcare system with blockchain technology. *Blockchain in Healthcare Today*, Forthcoming (2019)
73. Guennoun, M., El-Khatib, K.: Securing medical data in smart homes, pp. 104–107 (2009). <https://doi.org/10.1109/MEMEA.2009.5167964>
74. Guizani, K., Guizani, S.: IoT healthcare monitoring systems overview for elderly population, pp. 2005–2009 (2020)
75. Gupta, A., Bansiya, A.: Utilizing cloud computing for stronger healthcare data security. *Int. J. Sci. Res. Eng. Trends* **6**, 2384 (2020)
76. Gupta, V., Metha, G.: Medical data security using cryptography, pp. 866–869 (2018)
77. Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., El Koutbi, M.: Digging deeper into data breaches: an exploratory data analysis of hacking breaches over time. *Procedia Comput. Sci.* **151**, 1004–1009 (2019)
78. Hollis, K.F.: To share or not to share: ethical acquisition and use of medical data. *AMIA Summits Transl. Sci. Proc.* **2016**, 420 (2016)
79. Holmgren, A.J., Adler-Milstein, J.: Health information exchange in us hospitals: the current landscape and a path to improved information sharing. *J. Hospital Med.* **12**(3), 193–198 (2017)
80. Hsu, W.W.Q., Chan, E.W.Y., Zhang, Z.J., Lin, Z.X., Bian, Z.X., Wong, I.C.K.: Chinese medicine students' views on electronic prescribing: a survey in Hong Kong. *Eur. J. Integr. Med.* **7**(1), 47–54 (2015)
81. Huang, C.D., Behara, R.S., Goo, J.: Optimal information security investment in a healthcare information exchange: An economic analysis. *Decis. Support Syst.* **61**, 1–11 (2014)
82. Ibrahim, A., Mahmood, B., Singhal, M.: A secure framework for sharing electronic health records over clouds, pp. 1–8 (2016). <https://doi.org/10.1109/SeGAH.2016.7586273>
83. Ibrahim, A., Mahmood, B., Singhal, M.: A secure framework for sharing electronic health records over clouds, pp. 1–8 (2016)
84. Ivaşcu, T., Frîncu, M., Negru, V.: Considerations towards security and privacy in internet of things based ehealth applications, pp. 275–280 (2016). <https://doi.org/10.1109/SISY.2016.7601512>
85. Izza, S., Benssalah, M., Drouiche, K.: An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *J. Inf. Secur. Appl.* **58**, 102705 (2021)
86. Jabeen, T., Ashraf, H., Khatoun, A., Band, S.S., Mosavi, A.: A lightweight genetic based algorithm for data security in wireless body area networks. *IEEE Access* **8**, 183460–183469 (2020)
87. Jabeen, T., Ashraf, H., Ullah, A.: A survey on healthcare data security in wireless body area networks. *J. Ambient Intell. Humanized Comput.* 1–14 (2021)
88. Jaigirdar, F.T.: Trust based security solution for internet of things healthcare solution: an end-to-end trustworthy architecture, pp. 1757–1760 (2018)
89. Jalali, M.S., Razak, S., Gordon, W., Perakslis, E., Madnick, S.: Health care and cybersecurity: bibliometric analysis of the literature. *J. Med. Internet Res.* **21**(2), e12644 (2019)

90. Janjic, V., et al.: The serums tool-chain: Ensuring security and privacy of medical data in smart patient-centric healthcare systems, pp. 2726–2735 (2019)
91. Jayanthilladevi, A., Sangeetha, K., Balamurugan, E.: Healthcare biometrics security and regulations: biometrics data security and regulations governing PHI and HIPAA act for patient privacy, pp. 244–247 (2020)
92. Joshitta, R.S.M., Arockiam, L., Malarchelvi, P.S.K.: Security analysis of sat\_jo lightweight block cipher for data security in healthcare IoT, pp. 111–116 (2019)
93. Kamoun, F., Nicho, M.: Human and organizational factors of healthcare data breaches: the swiss cheese model of data breach causation and prevention. *Int. J. Healthcare Inf. Syst. Inf. (IJHISI)* **9**(1), 42–60 (2014)
94. Karthick, R., Ramkumar, R., Akram, M., Kumar, M.V.: Overcome the challenges in bio-medical instruments using IoT-a review. *Materials Today: Proceedings* (2020)
95. Kaur, J., et al.: Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: a design perspective. *Risk Manage. Healthcare Policy* **13**, 355 (2020)
96. Kausar, F.: Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Inf. J.* (2021)
97. Kaw, J.A., Loan, N.A., Parah, S.A., Muhammad, K., Sheikh, J.A., Bhat, G.M.: A reversible and secure patient information hiding system for IoT driven e-health. *Int. J. Inf. Manage.* **45**, 262–275 (2019)
98. Kelkar, V., Tuckley, K.: Reversible watermarking for medical images with added security using chaos theory, pp. 84–87 (2018). <https://doi.org/10.1109/CESYS.2018.8724039>
99. Kenny, G., O'Connor, Y., Eze, E., Ndibuagu, E., Heavin, C.: A ground-up approach to mHealth in Nigeria: a study of primary healthcare workers' attitude to mHealth adoption. *Procedia Comput. Sci.* **121**, 809–816 (2017)
100. Khaloufi, H., Abouelmehdi, K., Beni-hssane, A., Saadi, M.: Security model for big healthcare data lifecycle. *Procedia Comput. Sci.* **141**, 294–301 (2018)
101. Khan, F.A., Ali, A., Abbas, H., Haldar, N.A.H.: A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Comput. Sci.* **34**, 511–517 (2014)
102. Khan, J., et al.: Medical image encryption into smart healthcare IoT system, pp. 378–382 (2019). <https://doi.org/10.1109/ICCWAMTIP47768.2019.9067592>
103. Khan, J., et al.: Medical image encryption into smart healthcare IoT system, pp. 378–382 (2019)
104. Kierkegaard, P.: Medical data breaches: notification delayed is notification denied. *Comput. Law Secur. Rev.* **28**(2), 163–183 (2012)
105. Kim, J., Feng, D.D., Cai, T.W., Eberl, S.: Integrated multimedia medical data agent in e-health. In: *Proceedings of the Pan-Sydney area Workshop on Visual Information Processing*, vol. 11, pp. 11–15 (2001)
106. Kiourtis, A., Mavrogiorgou, A., Kyriazis, D., Graziani, A., Torelli, F.: Improving health information exchange through wireless communication protocols, pp. 32–39 (2020). <https://doi.org/10.1109/WiMob50308.2020.9253374>
107. Kiruba, W.M., Vijayalakshmi, M.: Implementation and analysis of data security in a real time IoT based healthcare application, pp. 1460–1465 (2018)
108. Ko, J., Lu, C., Srivastava, M.B., Stankovic, J.A., Terzis, A., Welsh, M.: Wireless sensor networks for healthcare. *Proc. IEEE* **98**(11), 1947–1960 (2010)
109. Kondawar, S.S., Gawali, D.H.: Security algorithms for wireless medical data, pp. 1–6 (2016)



110. Krishna, R., Kelleher, K., Stahlberg, E.: Patient confidentiality in the research use of clinical medical databases. *Am. J. Public Health* **97**(4), 654–658 (2007)
111. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., von Zezschwitz, E.: “If https Were Secure, i Wouldn’t need 2fa”-end User and Administrator Mental Models of https, pp. 246–263 (2019)
112. Kumar, M., Chand, S.: Medhypchain: a patient-centered interoperability hyperledger-based medical healthcare system: regulation in covid-19 pandemic. *J. Netw. Comput. Appl.* **179**, 102975 (2021)
113. Kumar, S., Namdeo, V.: Enabling privacy and security of healthcare-related data in the cloud
114. Kumar, V.N., Rochan, M., Hariharan, S., Rajamani, K.: Data hiding scheme for medical images using lossless code for mobile HIMS, pp. 1–4 (2011)
115. Kuo, M.H., Chrimess, D., Moa, B., Hu, W.: Design and construction of a big data analytics framework for health applications, pp. 631–636 (2015)
116. Lee, C.Y., Ibrahim, H., Othman, M., Yaakob, R.: Reconciling semantic conflicts in electronic patient data exchange, pp. 390–394 (2009)
117. Lees, P.J., Chronaki, C.E., Simantirakis, E.N., Kostomanolakis, S.G., Orphanoudakis, S.C., Vardas, P.E.: Remote access to medical records via the internet: feasibility, security and multilingual considerations, pp. 89–92 (1999). <https://doi.org/10.1109/CIC.1999.825913>
118. Li, P., Xu, C., Luo, Y., Cao, Y., Mathew, J., Ma, Y.: Carenet: building regulation-compliant home-based healthcare services with software-defined infrastructure, pp. 373–382 (2017)
119. Li, X., Huang, X., Li, C., Yu, R., Shu, L.: Edgecare: leveraging edge computing for collaborative data management in mobile healthcare systems. *IEEE Access* **7**, 22011–22025 (2019)
120. Liu, H., Kadir, A., Liu, J.: Color pathological image encryption algorithm using arithmetic over galois field and coupled hyper chaotic system. *Opt. Lasers Eng.* **122**, 123–133 (2019)
121. Lohiya, S., Ragha, L.: Privacy preserving in data mining using hybrid approach, pp. 743–746 (2012). <https://doi.org/10.1109/CICN.2012.166>
122. Lomotey, R.K., Pry, J., Sriramoju, S.: Wearable IoT data stream traceability in a distributed health information system. *Pervasive Mob. Comput.* **40**, 692–707 (2017)
123. Jones, J.M., Duezguen, R., Mayer, P., Volkamer, M., Das, S.: A literature review on virtual reality authentication. In: Furnell, S., Clarke, N. (eds.) HAISA 2021. IAICT, vol. 613, pp. 189–198. Springer, Cham (2021). [https://doi.org/10.1007/978-3-030-81111-2\\_16](https://doi.org/10.1007/978-3-030-81111-2_16)
124. Mahima, K.T.Y., Ginige, T.: A secured healthcare system using blockchain and graph theory (2020). <https://doi.org/10.1145/3440084.3441217>
125. Majam, T., Theron, F.: The purpose and relevance of a scientific literature review: a holistic approach to research. *J. Public Adm.* **41**(3), 603–615 (2006)
126. Maji, A.K., et al.: Security analysis and implementation of web-based telemedicine services with a four-tier architecture, pp. 46–54 (2008)
127. Majumdar, R., Das, S.: Sok: an evaluation of quantum authentication through systematic literature review. In: Proceedings of the Workshop on Usable Security and Privacy (USEC) (2021)
128. Mashima, D., Ahamad, M.: Enhancing accountability of electronic health record usage via patient-centric monitoring (2012). <https://doi.org/10.1145/2110363.2110410>



129. Masood, I., Wang, Y., Daud, A., Aljohani, N.R., Dawood, H.: Privacy management of patient physiological parameters. *Telematics Inf.* **35**(4), 677–701 (2018)
130. Masood, I., Wang, Y., Daud, A., Aljohani, N.R., Dawood, H.: Towards smart healthcare: patient data privacy and security in sensor-cloud infrastructure. *Wirel. Commun. Mob. Comput.* **2018** (2018)
131. Mbonihankuye, S., Nkuzimana, A., Ndagijimana, A.: Healthcare data security technology: hipaa compliance. *Wirel. Commun. Mob. Comput.* **2019** (2019)
132. McLeod, A., Dolezel, D.: Cyber-analytics: modeling factors associated with healthcare data breaches. *Decis. Support Syst.* **108**, 57–68 (2018)
133. Melchiorre, M.G., Papa, R., Rijken, M., van Ginneken, E., Hujala, A., Barbabella, F.: eHealth in integrated care programs for people with multimorbidity in Europe: insights from the ICARE4EU project. *Health Policy* **122**(1), 53–63 (2018)
134. Miah, S.J., Hasan, J., Gammack, J.G.: On-cloud healthcare clinic: an e-health consultancy approach for remote communities in a developing country. *Telematics Inf.* **34**(1), 311–322 (2017)
135. Mirto, M., Cafaro, M., Aloisio, G.: Peer-to-peer data discovery in health centers, pp. 343–348 (2013)
136. Mounia, B., Habiba, C.: Big data privacy in healthcare Moroccan context. *Procedia Comput. Sci.* **63**, 575–580 (2015)
137. Naseem, M.T., Qureshi, I.M., Muzaffar, M.Z., et al.: Robust watermarking for medical images resistant to geometric attacks, pp. 224–228 (2012). <https://doi.org/10.1109/INMIC.2012.6511496>
138. Nausheen, F., Begum, S.H.: Healthcare IoT: benefits, vulnerabilities and solutions, pp. 517–522 (2018)
139. Noah, N., Das, S.: Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. *Comput. Animation Virtual Worlds e2020* (2021)
140. Noel, K., Yagudayev, S., Messina, C., Schoenfeld, E., Hou, W., Kelly, G.: Tele-transitions of care. a 12-month, parallel-group, superiority randomized controlled trial protocol, evaluating the use of telehealth versus standard transitions of care in the prevention of avoidable hospital readmissions. *Contemp. Clin. Trials Commun.* **12**, 9–16 (2018)
141. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain Bus. *Inf. Syst. Eng.* **59**(3), 183–187 (2017)
142. Olaronke, I., Oluwaseun, O.: Big data in healthcare: Prospects, challenges and resolutions, pp. 1152–1157 (2016)
143. Pai, R.R., Alathur, S.: Determinants of mobile health application awareness and use in India: an empirical analysis, pp. 576–584 (2020)
144. Paksunemi, M., Sorvoja, H., Alasaarela, E., Myllyla, R.: Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit, pp. 5182–5185 (2006)
145. Palta, J.R., Frouhar, V.A., Dempsey, J.F.: Web-based submission, archive, and review of radiotherapy data for clinical quality assurance: a new paradigm. *Int. J. Radiat. Oncol.\* Biol.\* Phys.* **57**(5), 1427–1436 (2003)
146. Pandey, A.K., et al.: Key issues in healthcare data integrity: analysis and recommendations. *IEEE Access* **8**, 40612–40628 (2020)
147. Pandey, H.M.: Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. *Future Gener. Comput. Syst.* **111**, 213–225 (2020)

148. Parameswari, R., Latha, R.: Analysis of wavelet transform approach for healthcare data security in cloud framework. *Int. J. Sci. Res. Sci. Eng. Technol.* **2**, 241–246 (2016)
149. Parmar, M., Shah, S.: Reinforcing security of medical data using blockchain, pp. 1233–1239 (2019). <https://doi.org/10.1109/ICCS45141.2019.9065830>
150. Perumal, A.M., Nadar, E.R.S.: Architectural framework of a group key management system for enhancing e-healthcare data security. *Healthcare Technol. Lett.* **7**(1), 13–17 (2020)
151. Petković, M.: Remote patient monitoring: Information reliability challenges, pp. 295–301 (2009)
152. Pirbhulal, S., Samuel, O.W., Wu, W., Sangaiah, A.K., Li, G.: A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **95**, 382–391 (2019)
153. Pirbhulal, S., Shang, P., Wu, W., Sangaiah, A.K., Samuel, O.W., Li, G.: Fuzzy vault-based biometric security method for tele-health monitoring systems. *Comput. Electr. Eng.* **71**, 546–557 (2018)
154. Polap, D., Srivastava, G., Yu, K.: Agent architecture of an intelligent medical system based on federated learning and blockchain technology. *J. Inf. Secur. Appl.* **58**, 102748 (2021)
155. Polap, D., Srivastava, G., Jolfaei, A., Parizi, R.M.: Blockchain technology and neural networks for the internet of medical things, pp. 508–513 (2020). <https://doi.org/10.1109/INFOCOMWKSHP50562.2020.9162735>
156. PraveenKumar, R., Divya, P.: Medical data processing and prediction of future health condition using sensors data mining techniques and r programming. *Int. J. Sci. Res. Eng. Dev.* **3**(4) (2020)
157. Psarra, E., Patiniotakis, I., Verginadis, Y., Apostolou, D., Mentzas, G.: Securing access to healthcare data with context-aware policies, pp. 1–6 (2020)
158. Qazi, U., Haq, M., Rashad, N., Rashid, K., Ullah, S., Raza, U.: Availability and use of in-patient electronic health records in low resource setting. *Comput. Methods Program. Biomed.* **164**, 23–29 (2018)
159. Rajagopalan, S., Dhamodaran, B., Ramji, A., Francis, C., Venkatraman, S., Amirtharajan, R.: Confusion and diffusion on FPGA-Onchip solution for medical image security, pp. 1–6 (2017)
160. Reni, G., Molteni, M., Arlotti, S., Pinciroli, F.: Chief medical officer actions on information security in an Italian rehabilitation centre. *Int. J. Med. Inf.* **73**(3), 271–279 (2004)
161. del Rey, A.M., Pastora, J.H., Sánchez, G.R.: 3d medical data security protection. *Exp. Syst. Appl.* **54**, 379–386 (2016)
162. Richardson, J.E., Ancker, J.S.: Public perspectives of mobile phones' effects on healthcare quality and medical data security and privacy: A 2-year nationwide survey, vol. 2015, p. 1076 (2015)
163. Rocha, A., et al.: Innovations in health care services: the caalyx system. *Int. J. Med. Inf.* **82**(11), e307–e320 (2013)
164. Rodrigues, H.A.M., Antunes, L., Correia, M.E.: Proposal of a secure electronic prescription system, pp. 165–168 (2013)
165. Rodriguez-Colin, R., Claudia, F.D.J., Trinidad-Blas, G.: Data hiding scheme for medical images, pp. 32–32 (2007). <https://doi.org/10.1109/CONIELECOMP.2007.14>
166. Safkhani, M., Rostampour, S., Bendavid, Y., Bagheri, N.: IoT in medical & pharmaceutical: designing lightweight RFID security protocols for ensuring supply chain integrity. *Comput. Netw.* **181**, 107558 (2020)

167. Sammoud, A., Chalouf, M.A., Hamdi, O., Montavont, N., Bouallegue, A.: A new biometrics-based key establishment protocol in Wban: Energy efficiency and security robustness analysis. *Comput. Secur.* **96**, 101838 (2020)
168. Sartipi, K., Yarmand, M.H., Down, D.G.: Mined-knowledge and decision support services in electronic health, pp. 1–6 (2007)
169. Schmeelk, S.: Where is the risk? analysis of government reported patient medical data breaches, pp. 269–272 (2019)
170. Shaarani, I., et al.: Attitudes of patients towards digital information retrieval by their physician at point of care in an ambulatory setting. *Int. J. Med. Inf.* **130**, 103936 (2019)
171. Shahbaz, S., Mahmood, A., Anwar, Z.: Soad: securing oncology EMR by anonymizing DICOM images, pp. 125–130 (2013). <https://doi.org/10.1109/FIT.2013.30>
172. Shakil, K.A., Zareen, F.J., Alam, M., Jabin, S.: Bamhealthcloud: a biometric authentication and data management system for healthcare data in cloud. *J. King Saud Univ. Comput. Inf. Sci.* **32**(1), 57–64 (2020)
173. Shen, H., et al.: Miaps: a web-based system for remotely accessing and presenting medical images. *Comput. Methods Program. Biomed.* **113**(1), 266–283 (2014)
174. Shere, A.R., Nurse, J.R., Flechais, I.: Security should be there by default: investigating how journalists perceive and respond to risks from the internet of things, pp. 240–249 (2020)
175. Shi, W., Dustdar, S.: The promise of edge computing. *Computer* **49**(5), 78–81 (2016)
176. Shrivastava, S., Srikanth, T., VS, D.: e-Governance for healthcare service delivery in India: challenges and opportunities in security and privacy, pp. 180–183 (2020)
177. Shrivastava, U., Song, J., Han, B.T., Dietzman, D.: Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? a cross-country investigation. *Int. J. Med. Inf.* **148**, 104401 (2021)
178. da Silva Etges, A.P.B., et al.: Development of an enterprise risk inventory for healthcare. *BMC Health Serv. Res.* **18**(1), 1–16 (2018)
179. Simões, A., et al.: Participatory implementation of an antibiotic stewardship programme supported by an innovative surveillance and clinical decision-support system. *J. Hosp. Infect.* **100**(3), 257–264 (2018)
180. Simplicio, M.A., Iwaya, L.H., Barros, B.M., Carvalho, T.C., Näslund, M.: Secourhealth: a delay-tolerant security framework for mobile health data collection. *IEEE J. Biomed. Health Inf.* **19**(2), 761–772 (2014)
181. Sosu, R.N.A., Quist-Aphetsi, K., Nana, L.: A decentralized cryptographic blockchain approach for health information system, pp. 120–1204 (2019). <https://doi.org/10.1109/ICCMA.2019.00027>
182. Soualmi, A., Alti, A., Laouamer, L.: A blind image watermarking method for personal medical data security, pp. 1–5 (2019). <https://doi.org/10.1109/ICNAS.2019.8807442>
183. Sreeji, S., Shiji, S., Vysagh, M., Amma, T.A.: Security and privacy preserving deep learning framework that protect healthcare data breaches. *Int. J. Res. Eng. Sci. Manage.* **3**(7), 148–152 (2020)
184. Stobert, E., Barrera, D., Homier, V., Kollek, D.: Understanding cybersecurity practices in emergency departments, pp. 1–8 (2020)
185. Stowell, E., et al.: Designing and evaluating mhealth interventions for vulnerable populations: a systematic review, pp. 1–17 (2018)

186. Sudha, G., Ganesan, R.: Secure transmission medical data for pervasive healthcare system using android, pp. 433–436 (2013)
187. Sutton, L.N.: PACS and diagnostic imaging service delivery-A UK perspective. *Eur. J. Radiol.* **78**(2), 243–249 (2011)
188. Tan, C.C., Wang, H., Zhong, S., Li, Q.: Body sensor network security: an identity-based cryptography approach, pp. 148–153 (2008)
189. Tan, C.C., Wang, H., Zhong, S., Li, Q.: Ibe-lite: a lightweight identity-based cryptography for body sensor networks. *IEEE Trans. Inf. Technol. Biomed.* **13**(6), 926–932 (2009)
190. Thamilarasu, G., Lakin, C.: A security framework for mobile health applications, pp. 221–226 (2017). <https://doi.org/10.1109/FiCloudW.2017.96>
191. Tian, Y., et al.: Popcorn: a web service for individual prognosis prediction based on multi-center clinical data collaboration without patient-level data sharing. *J. Biomed. Inf.* **86**, 1–14 (2018)
192. Tolba, A., Al-Makhadmeh, Z.: Predictive data analysis approach for securing medical data in smart grid healthcare systems. *Future Gener. Comput. Syst.* **117**, 87–96 (2021)
193. Tyler, J.L.: The healthcare information technology context: a framework for viewing legal aspects of telemedicine and teleradiology, pp. 1–10 (2001)
194. U.S. Department of Health & Human Services: Anthem pays OCR \$16 Million in record HIPAA settlement following largest health data breach in history, 15 Oct 2018. <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html>
195. Usman, M.A., Usman, M.R.: Using image steganography for providing enhanced medical data security, pp. 1–4 (2018). <https://doi.org/10.1109/CCNC.2018.8319263>
196. Uy, R.C.Y., Kury, F.S., Fontelo, P.: Wireless networks, physician handhelds use, and medical devices in us hospitals, pp. 1–6 (2015)
197. Vallathan, G., Rajamani, V., Harinee, M.P.: Enhanced medical data security and perceptual quality for healthcare services, pp. 1–6 (2020). <https://doi.org/10.1109/ICSCAN49426.2020.9262309>
198. Vassis, D., Belsis, P., Skourlas, C.: Secure management of medical data in wireless environments, pp. 427–432 (2012)
199. Véliz, C.: Not the doctor's business: privacy, personal responsibility and data rights in medical settings. *Bioethics* **34**(7), 712–718 (2020)
200. Vidya, M., Padmaja, K.: Enhancing security of electronic patient record using watermarking technique. *Mater. Today Proc.* **5**(4), 10660–10664 (2018)
201. Vijayalakshmi, A.V., Arockiam, L.: Hybrid security techniques to protect sensitive data in e-healthcare systems, pp. 39–43 (2018)
202. Wagner, P.: Third party breaches-a survey of threats and recommendations, SSRN 3782822 (2021)
203. Walker-Roberts, S., Hammoudeh, M., Dehghantanha, A.: A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access* **6**, 25167–25177 (2018)
204. Wang, C.X.: Security issues to tele-medicine system design, pp. 106–109 (1999)
205. Wang, D., Kale, S.D., O'Neill, J.: Please call the specialism: Using wechat to support patient care in china, pp. 1–13 (2020)
206. Wang, D., Huang, Q., Chen, X., Ji, L.: Location of three-dimensional movement for a human using a wearable multi-node instrument implemented by wireless body area networks. *Comput. Commun.* **153**, 34–41 (2020)

207. Weaver, A.C., et al.: Federated, secure trust networks for distributed healthcare it services, pp. 162–169 (2003). <https://doi.org/10.1109/INDIN.2003.1300264>
208. Yaghmai, V., Salehi, S.A., Kuppaswami, S., Berlin, J.W.: Rapid wireless transmission of head CT images to a personal digital assistant for remote consultation. *Acad. Radiol.* **11**(11), 1291–1293 (2004)
209. Yang, W., et al.: Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. *IEEE Access* **6**, 36939–36947 (2018)
210. Yang, Y., Xiao, X., Cai, X., Zhang, W.: A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access* **7**, 96900–96911 (2019)
211. Yang, Y., Xiao, X., Cai, X., Zhang, W.: A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access* **7**, 96900–96911 (2019). <https://doi.org/10.1109/ACCESS.2019.2929298>
212. Yesmin, T., Carter, M.W.: Evaluation framework for automatic privacy auditing tools for hospital data breach detections: a case study. *Int. J. Med. Inf.* **138**, 104123 (2020)
213. Zatout, Y., Campo, E., Llibre, J.F.: Toward hybrid WSN architectures for monitoring people at home, pp. 308–314 (2009). <https://doi.org/10.1145/1643823.1643880>
214. Zhang, B., Chen, S., Nichols, E., D’Souza, W., Prado, K., Yi, B.: A practical cyberattack contingency plan for radiation oncology. *J. Appl. Clin. Med. Phys.* **21**(7), 181–186 (2020)