Scientific Research Publishing

E-Health Telecommunication Systems and Networks, 2024, 13, 23-44
https://www.scirp.org/journal/etsn
ISSN Online: 2167-9525
ISSN Print: 2167-9517

A Literature Review: Potential Effects That Health Apps on Mobile Devices May Have on Patient Privacy and Confidentiality

Anna Sheri George*, Jomin George, Judy Jenkins

Faculty of Medicine and Health Life Sciences, Swansea University, Swansea, UK
Email: *annageorgeswansea@gmail.com

How to cite this paper: George, A.S., George, J. and Jenkins, J. (2024) A Literature Review: Potential Effects That Health Apps on Mobile Devices May Have on Patient Privacy and Confidentiality. *E-Health Telecommunication Systems and Networks*, **13**, 23-44.
https://doi.org/10.4236/etsn.2024.133003

Received: February 29, 2024
Accepted: August 6, 2024
Published: August 9, 2024

Abstract

Purpose: This research aims to evaluate the potential threats to patient privacy and confidentiality posed by mHealth applications on mobile devices. **Methodology:** A comprehensive literature review was conducted, selecting eighty-eight articles published over the past fifteen years. The study assessed data gathering and storage practices, regulatory adherence, legal structures, consent procedures, user education, and strategies to mitigate risks. **Results:** The findings reveal significant advancements in technologies designed to safeguard privacy and facilitate the widespread use of mHealth apps. However, persistent ethical issues related to privacy remain largely unchanged despite these technological strides.

Keywords

Mobile Devices, Patient Privacy, Confidentiality Breaches, Data Security, Data Protection, Regulatory Compliance, User Consent, Data Encryption, Third-Party Integration, User Awareness

1. Introduction

mHealth, or mobile health, represents a subset of eHealth that leverages smartphones, tablets, and other mobile devices to enhance healthcare delivery. Over the years, mHealth has gained traction due to its potential to address healthcare accessibility issues, reduce costs, and improve patient engagement.

mHealth or mobile health, a subset of eHealth, is related to the idea of utilizing smartphones, tablets, and mobile phones within fields of medicine, for better delivery of health care [1]. Mobile healthcare focuses on the use of wireless communication, computers to process data, and sensing gadgets to manage the delivery of healthcare devices [2]. Cell phones came into the market many years ago and

the number of mobile health (mHealth) apps marked a growing surge [3]. The access to the clinical diagnosis and treatment that mHealth apps made possible for many people using cell phones, across the world is remarkable [4]. Health apps were taken up by the health care field to sort many of the issues like the unavailability of health services in rural or remote areas, to reduce the high cost of essential health care to the patients, and, to reduce the difficulties in organizing or scheduling an appointment with a specialist for people living in isolated areas [5]. The main aim of mHealth apps is to make more of the patient's involvement by guiding them positively for better results regarding their health, which will in turn help the patients to have power and control over their health [4].

In the study done by [1], most of the mHealth apps were available free of cost to the consumers, and half of the people who owned smartphones used their phones to check health information while a few of them had an app downloaded peculiarly for managing their health. In 2021, there was a global increase in the number of apps downloaded compared to 2020, due to the availability of internet [6]; similarly, the number of apps that were available in March 2020 has expanded by 200 daily in the market [7].

Mobile health apps were used widely during the first 10 years of the 21st century which led to a rise in the time people invest in improving their health and it necessitated the use of a digital environment by most health industries [8]. Despite all the unputdownable benefits, mHealth apps have several challenges and limitations including data breaches and security risks, inadequate encryption, third-party data sharing, Identity theft, and lack of regulatory compliance [9]. Four major drawbacks that users identified with mHealth apps were related to reliability, suitability, customization, and usability [10]. Checking the quality and safety of mHealth apps is of great interest since, health apps have possible risks associated with them [7]. mHealth app users are generally aware of the risks associated with the use of mobile health applications and users still choose to use the technological advancements [11].

The adoption of mHealth apps has surged, with many being offered free of charge. Studies indicate that a significant portion of smartphone users utilize these apps to manage their health. The COVID-19 pandemic further accelerated the uptake of mHealth apps, with a notable increase in downloads and usage. Despite the benefits, mHealth apps face several challenges, including data breaches, inadequate encryption, third-party data sharing, identity theft, and lack of regulatory compliance. User concerns often revolve around reliability, customization, and usability of these apps. This paper aims to address the persistent privacy and confidentiality issues associated with mHealth applications. By reviewing the existing literature, we seek to identify common problems and propose solutions to enhance data security and user trust in mHealth technologies.

2. Methods

2.1. Search Strategy

A search was conducted across PubMed, ScienceDirect, ResearchGate, and Se-

matic Scholar databases, focusing on the past fifteen years from 2007 to 2023. This timeframe was chosen to ensure recent literature representation while allowing for the observation of how issues have evolved over time with technological advancements. Limiting the search to five or ten years is deemed excessively restrictive, as it would overlook this historical development of these issues.

Relevant search terms such as *mobile devices*, *patient privacy*, *confidentiality breaches*, *data security*, *data protection*, *regulatory compliance*, *user consent*, *data encryption*, *third-party integration*, *and user awareness* were utilized to encompass the subject comprehensively. The use of Boolean operations like OR and AND facilitated the broadest possible retrieval of relevant articles. Articles were then categorized into common problems and proposed solutions.

2.2. Selection

We opted to review a total of eighty-eight articles sourced from diverse geographical locations across various countries because, we view health information as a fundamental requirement for all individuals and acknowledge the global significance on privacy and confidentiality with use of mHealth apps (Table 1). Incorporating studies from various countries was deemed suitable to pinpoint both shared patterns and disparities, thus offering a comprehensive overview of the literature concerning this subject.

Table 1. Articles on privacy and confidentiality with use of mHealth apps.

Author	Engineering Framework	Password Protection	Data Encryption	Privacy Regulation	Unsecured Connections	Ownership and Storage	User Behaviour	Law Enforcement
Aljedaani *et al.*, 2023							Y	
Alsyouf *et al.*, 2023							Y	
Ammar *et al.*, 2021						Y		
Aydin, 2023							Y	
Benaloh *et al.*, 2009						Y		
Benjumea *et al.*, 2020	Y			Y				
Boyles *et al.*, 2012							Y	
Braghin *et al.*, 2018			Y					
Cano & Esplugues, 2023								
Chatzipavlou *et al.*, 2016	Y							
Coiera, 2015								
Cyrkel, 2018						Y		
Dagher *et al.*, 2018							Y	
Daley *et al.*, 2022			Y					
Deebak *et al.*, 2019		Y						
Dicianno *et al.*, 2015								

Continued

Ducato, 2016								Y
Egala *et al.*, 2021		Y						
Enamamu *et al.*, 2020		Y						
Galvin and DeMuro, 2020	Y			Y				
Greene *et al.*, 2019						Y		
Gurupur and Wan, 2017						Y		Y
Hasan *et al.*, 2021		Y						
Hathaliya and Tanwar, 2017						Y		
He *et al.*, 2014					Y			Y
Hendricks, 2022								Y
Hilty *et al.*, 2019							Y	
Huh, 2020								
Hussain *et al.*, 2018								
Islam, 2022					Y			
Jaeger *et al.*, 2016			Y					
Jain, 2023								Y
Jules and Ristenpart, 2014			Y					
Jusob er al., 2017								
Jusob *et al.*, 2022	Y							
Kharrazi *et al.*, 2012		Y						
Knorr and Aspinall, 2015								Y
Kotz *et al.*, 2016								Y
Larson, 2018								
Mancinini, 2023								Y
Martinez-Perez *et al.*, 2015		Y						Y
Mia *et al.*, 2022			Y					Y
Morera *et al.*, 2016		Y						
Mustafa *et al.*, 2019		Y	Y				Y	Y
Nagaraj *et al.*, 2015			Y					
Nouri *et al.*, 2018								
Nurgalieva *et al.*, 2020								Y
Olivia *et al.*, 2022								Y
O'Loughlin *et al.*, 2019				Y				

Continued

Palos-Sanchez *et al.*, 2021								
Parker *et al.*, 2019				Y				
Plachkinova *et al.*, 2015							Y	
Rajput *et al.*, 2023	Y		Y					
Ren *et al.*, 2016						Y		
Roberts *et al.*, 2021								
Robillard *et al.*, 2019				Y				
Sampat *et al.*, 2020								
Saracevic *et al.*, 2020	Y		Y					
Sardi *et al.*, 2020				Y				
Schroeder *et al.*, 2022							Y	
Scott *et al.*, 2015								
Shafique *et al.*, 2017		Y						
Shemesh and Barnoy, 2020							Y	
Shipp and Blasco, 2020				Y				
Shu and Jahankhani, 2017								Y
Shuwandy *et al.*, 2020			Y					
Silva *et al.*, 2013			Y					
Srivastava and Tamilarasu, 2019	Y							
Sunyaev *et al.*, 2015				Y				
Tangari *et al.*, 2021								Y
Tan *et al.*, 2021		Y	Y					
Thabit, 2019			Y					
Thamilarasu and Lakin, 2017	Y							
Tung, 2021								Y
Van *et al.*, 2019			Y				Y	
Vithanwattana *et al.*, 2017	Y	Y						
Vo *et al.*, 2019								
Yahya *et al.*, 2016								
Yarbrough and Smith, 2007							Y	
Zhou *et al.*, 2019		Y		Y			Y	
Zhou and Parmanto, 2020		Y					Y	
Zhu *et al.*, 2021		Y		Y				

3. Results

This literature review on the impact of mHealth apps on privacy and confidentiality reveals a multifaceted landscape characterized by both benefits and challenges. Several studies have underscored the potential of mHealth apps to empower patients by providing them with convenient access to healthcare services and information while promoting self-management of their healthcare services and information while promoting self-management of their health. This review reveals three main themes: the advantages and disadvantages of technology used for mHealth apps, user behavior, and law enforcement for patient data privacy and confidentiality. Within the theme of technology, several sub-themes emerged.

Firstly, an engineering framework for data security is paramount to ensuring the confidentiality of patient information. Studies emphasize the importance of robust security measures, such as encryption protocols and secure authentication methods, to safeguard sensitive data from unauthorized access or breaches.

Secondly, securing access using password and verifying identity is crucial for protecting patient privacy. Research underscores the significance of implementing strong authentication mechanisms to prevent unauthorized users from accessing mHealth apps and the sensitive data they contain.

Thirdly, data encryption plays a pivotal role in safeguarding patient information from interception or unauthorized access during transmission and storage. Studies emphasize the need for robust encryption protocols to ensure that patient data remains confidential and protected from cyber-attacks.

Moreover, privacy regulations for mobile health applications are essential for establishing clear guidelines and standards for data protection. Additionally, the use of unsecured public Wi-Fi connections poses a significant risk to patient privacy, as it increases the vulnerability of data transmission to interception or hacking. Studies emphasize the importance of educating users about the risks associated with using public Wi-Fi and implementing measures to mitigate the risk.

Lastly, issues related to data ownership and storage raise concerns about the control and access rights over patient information stored within mHealth apps. Research suggests the need for transparent policies regarding data ownership and storage practices to ensure that patient retains control over their personal health information.

3.1. Advantages and Weaknesses of Technology Utilized with mHealth Applications

Mobile health (mHealth) applications have revolutionized the interaction between physicians and patients [12]. Instances of data breaches are increasingly common and cause greater financial harm to numerous businesses [13] by involving significant disclosure of sensitive data to external organizations, causing subsequent actions like inquiries, rectifications, and legal costs [14].

Starting from 2005, the frequency of data breaches has increased by over three times, largely due to technological advancements and the dissemination of information [15]. Concerns about data privacy were a recent concept for both developers and users [16], also, technological advancements in Mobile cloud computing and cloud-based Electronic Health Records (EHRs) have provided remedies for the security of devices and maintained data secrecy to a certain extent [17].

3.1.1. Engineering Frameworks for Data Security

A privacy framework outlines fundamental principles, methodologies, and solutions for safeguarding individuals' personal information and privacy, and therefore setting up an appropriate framework for mHealth is required to promote patient trust [18] [19]. A significant role in the liaison of mHealth apps is played by transport security and the possibility of a data breach happens while reading data via a proxy server, from which the application takes data and displays it for patients [20]. Under the data protection laws of the United Kingdom, data collected from a mobile health app is considered sensitive personal information which provides details about their health system and for the same reason it is essential to maintain data security on mobile devices and when it is transferred to a storage facility [21]. Because of the large volume of users' sensitive health data and to safeguard the privacy of its citizens, governments have developed frameworks [16].

[22] mentioned that having a framework serves as a foundation and key element for information security in mHealth systems. Various efforts were made to form security frameworks in the past, yet none have had essential functions of security, ethics, and availability [21]. The scan conducted by [23] unveiled many weaknesses within the 15 medical android applications of which, a significant portion could have been averted by better coding practices and secure engineering; also, he puts forward the idea that the responsibility is on the developer to remain updated about current security protocols and standards.

mHealth security frameworks effectiveness was assessed by [24] who found that security frameworks can be incorporated into any health app seamlessly to reduce security and privacy risks without compromising the user experience and the effects of using security frameworks were remarkable regarding security and privacy. Combining mHealth with blockchain technology provided an effective solution to ensure the easiness of accessing data and transparency [25] [26]. The global regulatory framework influenced by the General Data Protection Regulation (GDPR) defines data concerning the individual granting additional rights to users, to object, process, and erase [27].

3.1.2. Securing Access Using Passwords and Verifying Identity

[28] refers security as a condition to protect patients' health information from unauthorized use and privacy means the absence of unapproved trespasses. Intrusions can happen locally as well as remotely [29] and one of the security fea-

tures available to block remote intrusions, is multifactor authentication [30]-[32]. In the study conducted by [33], nineteen independent mobile personal health records (mPHR) were assessed with emphasis on the significance of data security, data import and export capabilities, image uploading and the opinion to generate a summary of health data found that, security and data privacy as significant concerns where the authors suggest having an additional layer of security using app-level passwords.

Devices with personal information must have suitable security measures to secure the data from fraud attacks [34]. Most health applications use a Single Factor Authentication (SFA) technique where, access to mHealth apps is protected by a password whereas, it has many limitations [35] [36]. Typically, users save their login details for apps on their mobile devices, making it simple for attackers to gain unauthorized access to sensitive data [21]. Even though the SFA method is more user-friendly, Two Factor Authentication (2FA) introduces additional elements to secure access to personal information [37]. 2FA, three-factor verification comprising Biometric Authentication and Grid-based Authentication approaches are the solutions introduced recently in the field of mHealth, to overcome the limitations of SFA [36]-[38].

Due to the seamless connectivity and the built-in sensors available in smart devices, it has been an advantage to extract biometric details needed to implement user authentication for mHealth apps [39] [40]. Utilizing the device authentication mechanism to confirm identity helped to prevent any unauthorized participation of devices and enhanced securing the privacy and confidentiality of personal information [41].

3.1.3. Data Encryption in Protecting Patient Information

Authentication for health apps based on password were susceptible to data breach and even alternate solutions of using biometric data and One-Time Password (OTP) for authentication also remained vulnerable to cyber-attacks [36]. For storing information securely and transferring without risks, Cryptography along with authentication serves as an effective solution, and the fundamental keys of cryptographic methods are encryption—responsible for converting data to an unintelligible form from its original state, and the decryption process—managing restoration of original data at the recipient's end by utilizing a confidential key [26] [42]. Information collected from an app must be encrypted from end-to-end to block unapproved access during the storage and transfer of data [34] [43] [44] in their comparative analysis, found encryption and decryption ensure the security of data even if a mobile phone with the mHealth app is robbed because theft of encrypted personal health data is challenging.

Numerous mHealth applications that lack utilizing encryption standards [45], which are considered at high risk for causing a significant threat to the privacy of patients' data, at the same time, those applications with encryption protocols have a very low risk for cyber-attacks [20] [46].

Conventional password-based authentication and encryption methods are not

sufficient for ensuring the security of healthcare data [47]. One of the most popular Password-based encryption (PBE) methods becomes vulnerable to cyber threats when users choose weak and easily predictable passwords making it easy for an attacker to decrypt if provided with encrypted plain text [48]. This issue is tackled with the use of Honey Encryption (HE) in which the encrypted plain text when decrypted with an invalid key reveals a valid yet false message, making it a challenge for the attacker to determine, if decryption was successful [48] [49].

One of the crucial and necessary functions to be employed by an app developer, for data gathering, storing, and transferring health information, is data encryption [49] [50].

3.1.4. Privacy Regulations for Mobile Health Applications

The privacy of a health application can be assessed by its privacy policy which gives details about the control, generation, processing, transfers, and storage of data; as well as acknowledgment of potential risks related to gathering data and users' rights, including the ability to cancel the consent [16] [51]. Recent studies reveal, a lack of privacy policy in frequently used mHealth apps due to the neglect of many developers [52]-[55]. It is even found that, at times, the privacy policy is not complete or exhaustingly large to read causing adverse outcomes of data breaches [54] [56]. In the same manner, health applications were lacking consumer consent, because there was no privacy policy, or the provided text was too lengthy for the users to understand [27]. On one hand, privacy policies do not give importance to the app by not providing enough information to end-users, and on the other hand, consumers are inclined to use apps with privacy policies that are not clear to them [57].

The focus of the designers for privacy policy should be on enhancing clarity by making it simple and emphasizing transparency which will make the privacy policy an effective one, and accordingly, it can lessen users' anxiety regarding privacy, boost their confidence, and improve their understanding of the advantages of utilizing health applications [51]. It must be explicitly mentioned in the policy if the data is shared for advertising purposes, and emphasis must be on its accessibility, whether in the app itself or the app store, and the users must be adequately informed about the ways the data is handled [58]. Similarly, the study done by [53] found the necessity to have details in the privacy policy, on the ways to report grievances regarding the app's privacy techniques. It is recommended in the study done by [52] that, before recommending a health app to the user, clinicians must assess its privacy policy for crucial details such as data encryption, safeguarding with passwords, and the capability to modify or erase details entered into the application.

3.1.5. Unsecured Public Wi-Fi Connections

To monitor and document the ongoing status or actions of the condition of a patient, certain mobile applications utilize the internet with the assistance of built-in sensors and this practice may pose a potential security risk [59]. The

study done by [60], found that most of the health apps are allowed to connect to the internet and are permitted to show advertisements; meanwhile, a few of them utilize it for transferring users' data via the internet. Data theft caused by unsecured connections can be managed by verifying user credentials and by making use of Transport Layer Security (TLS) or Secure Socket Layer (SSL) for safe connection on the internet [59] [60]. Furthermore, [60] suggests an in-depth review of external services for storing the users' sensitive data, and users must be notified when involving third-party, even if the network is secure and encrypted.

3.1.6. Data Ownership and Storage

There are two terms to be considered while discussing data ownership and they are, data owner—an individual or a person who generates health data referred to as a patient and, data consumer—a person, to whom the data owner wishes to exchange the personal health information with [61]. Granting patients complete control of their digital data ensures authentic ownership, privacy, and openness which will establish trust with patients using health applications [62]. Yet, [63] mentioned that it is difficult to determine the ownership of health data because the developers who made this advancement in the health sector also take part in the collection and usability of data. For patients to switch healthcare providers or to reassess their information and to even withdraw data access; "owner-driven access" for the patients enables them to decide on handling their data [61].

To distribute health information from data controllers to consumers, it is necessary to store the data in a database, and each information entered into the database is called a "record" [61]. Due to the vulnerability of information gathered through mHealth apps, it is a risk to store the data locally; even the traditional storage method of cloud computing had to face incidents of a breach in security [63]-[66]. Some of the challenges in the cloud computing model are also related to storage sites and creating backups of essential data as a precaution during data loss [64]. Remedies proposed for solving challenges in cloud computing involve saving health information as blocks of data without keeping an identity tag of the person who owns data, encrypting the data during collection, storage, and transmission [66] [67], finding the location of storage, modifying app features by evaluating usability and trustworthiness, and using the updated standards of interoperability [64].

3.2. User's Behavior

Extensively large amount of available mHealth applications poses considerable challenges for the users who lack awareness about the management and utilization of personal health information data [68] [69]. To understand how patients utilize technologies in the personal health record framework, [70] used Technology Acceptance Model (TAM) and found three main factors affected the usage: "Perceived Ease of Use (PEOU)"—utilization requires no extra effort of user, "Perceived Usefulness (PU)"—technology can offer advantages compared to existing methods [71], and the tendency to use the app by its security. Most peo-

ple use mHealth services when it is suggested by social friends or at times, due to the wide use of apps by everyone [43] [72], and most of the time, users are less worried about the confidentiality of their health data [11] [73]. The majority of the users of mHealth apps believed that applications from famous brands can be trusted when compared to others; on the other hand, people with knowledge of technology recommended features of encryption and participants with no IT knowledge highlighted the importance of ensuring the need of masking the identity of the individual in the users' group [43] [68] [74] mentioned that clinicians must evaluate the compatibility of the chosen technology and advise the use only to those who need it because it is crucial to employ the correct technology for the needed one at the right moment. Even though the use of good standards of security features protects the privacy of users, it is equally important to improve the awareness about security among people using health apps; so that the features are utilized effectively to safeguard their personal data [55] [68].

Intrusions that happen locally are privacy breaches done by people around a user; by inquiring about personal matters, unauthorized use of personal devices, or examining browsing history on their personal gadget [75]. To reduce these concerns and to motivate the use of mHealth apps, one strategy to incorporate is password protection and authentication [38].

When using public Wi-Fi connections with doubtful security or skeptical about the involvement of third-party, it is suggested that utilization of Hypertext Transfer Protocol Secure (HTTPS) and Virtual Private Network (VPN) enable encryption and secure communication enhancing the data privacy and confidentiality [34].

A user-friendly privacy safeguard integrated into mHealth applications is the use of generic names for the app because, some of the health applications choose to have their name pointed towards the disorder, which makes it easy for the people to figure out the kind of disorder the user is having; in such cases, as a security measure, users positioned these apps in a different folder with uncommon name [38].

3.3. Law Enforcement for Patient Data Privacy and Confidentiality

Even though mHealth applications are governed by regulations, like General Data Protection (GDPR) in European nations and Health Insurance Probability and Accountability (HIPPA) in the United States, more than half of the free mHealth app users are not informed about the data processing, which is necessary as per the regulatory guidelines, in one of the studies done by [76]. Similarly, many mHealth apps don't follow the law regulations making them vulnerable to privacy and security breaches [60] [64]. The study by [77] mentioned that regulations for data security and privacy of health apps could delay their usage within the medical field and it is confusing to differentiate between legal regulations needed for clinical apps and behavioral apps. However, the health sector specifically has become the prime target of data breaches due to the sensitive de-

tails given to medical records; including names, addresses, and even social security numbers [78] [79].

Even though individual nations maintain their separate frameworks for the protection and handling of sensitive health information, key aspects of consent, de-identification, and individual rights are commonly shared among countries in the West [80]; but existing regulations in developing countries do not cover digital health or have a sufficient law about data protection [81]. The main loophole is that regulations like HIPAA and GDPR aim to protect privacy with a focus on healthcare institutions and there has been limited attention given to the construction of secure mHealth apps with appropriate guidance [82] [83].

To accomplish the goals of protecting the privacy of patient data, GDPR ensured the implementation of adequate measures of the right to information, penalties from organizations and compensations to data owners for non-compliance, need for authorization for data handling, instant notification in case of a data breach, and clearly stated consent from users for collecting, storing, and transferring sensitive information [34] [84]-[86]. Furthermore, to overcome the challenges, it is advised to conduct regular external audits to assess the health app's compliance with policies and law regulations and update the laws specifically about data security due to the continuous expansion of technology used by the mobile health app industry [31] [87]. Applications that are non-compliant with the federal regulations' basic privacy requirements are barred from being deployed for the public and enable companies to rectify errors so that the applications are more secure [87].

Business partners developing the mHealth app for healthcare entities must adhere to the guidelines outlined by HIPPA such as administrative, technological, and safeguard measures to protect electronic health data [44]. In addition, patients should receive detailed information regarding privacy protocols in mHealth apps and the privacy hazards of using health apps before installing and utilizing them [88]. HIPAA regulations strongly recommend using informed consent from users, if personal data is required for research studies or for advertisement purposes; and in most cases, users are given the right to limit or refuse the utilization of their personal information regarding health, which to some extent help to protect privacy and confidentiality [80].

4. Discussion

The importance of privacy frameworks in mHealth is understood by their role in safeguarding personal information and fostering patient trust. Transport security is critical in preventing data breaches, especially when data is transmitted via proxy servers. Establishing security frameworks is fundamental for information security in mHealth systems, yet past efforts often lacked essential functions. Weakness in medical Android applications highlights the importance of secure coding practices and developer awareness of security protocols. Studies show that integrating security frameworks into health apps can significantly reduce risks without compromising user experience. Block chain technology combined

with mHealth offers transparency and ease of data access. Global regulatory framework, influenced by GDPR, grants users' additional rights over their data. Overall, effective privacy frameworks are vital for maintaining the security and privacy of mHealth data while ensuring regulatory compliance and user trust.

Security in mHealth involves protecting patient health information from unauthorized access, while privacy entails preventing unapproved intrusions, both locally and remotely. Multifactor authentication is a crucial security feature to block remote intrusions. Assessment of mobile personal health records highlights the significance of data security, with suggestions for additional security layers like app-level passwords. SFA has limitations, as saved login details on device make unauthorized access easier. 2FA, including Biometric Authentication and Grid-based authentication, addresses these limitations. Biometric details from smart devices aid seamless user authentication, enhancing privacy and confidentiality. Leveraging device authentication mechanisms further prevents unauthorized access, bolstering data security in mHealth applications.

Health apps' authentication methods, including biometric data and OTP, remain vulnerable to cyber-attacks. Cryptography, encompassing encryption and decryption, ensures secure data storage and transfer. Encryption is vital to prevent unauthorized access, with encryption data posing challenges even if the device is stolen. Applications lacking encryption standards pose a high risk to patient data privacy, while those with encryption protocols are less vulnerable to cyber threats. Conventional password-based encryption is insufficient, leading to the adoption of Honey Encryption, thwarting attackers with false decryption outcomes. App developers must prioritize data encryption for healthcare information security.

Assessing a health apps' privacy involves examining its policy, detailing data control, processing, and user rights. Many apps lack or have inadequate policies, increasing the risk of data breaches and user confusion. Privacy policies should prioritize clarity and transparency, simplifying language and emphasizing data handling practices, including advertising disclosures. Users should have easy access to policies and clear avenues for reporting privacy concerns. Clinicians should evaluate apps' policies before recommending them, focusing on encryption, password protection, and data modification capabilities. Enhancing privacy policies can alleviate user anxiety, enhance confidence, and promote app utilization.

Health apps often utilize the internet for data transfer, potentially posing security risks like data theft. User verification and encryption protocols like TLS and SSL can mitigate these risks. External services storing sensitive data should undergo thorough review, with users notified of third-party involvement even in secure networks.

Data ownership in healthcare involves the data owner and data consumer, with patient control fostering trust. However, ownership determination is complex due to developer involvement in data collection. Owner-driven access empowers patients to manage their data. Storing health data as records in database

poses security risks, exacerbated by breaches in local and cloud storage. Remedies include encryption data, evaluating app usability and trustworthiness, adhering to interoperability standards, and implementing blockchain for secure, decentralized storage without personal identifiers. These measures aim to address challenges in cloud computing and ensure data security and privacy in mHealth applications.

The abundance of mHealth apps poses challenges for users' data management awareness. Technology Acceptance Model highlights ease of use, usefulness, and security as key factor influencing app adoption. Improving security awareness is crucial alongside implementing security features like password protection. Locally, privacy breaches occur through personal intrusions, mitigated by password protection. Using HTTPS and VPN on public Wi-Fi enhances data privacy. Generic app names enhance privacy by concealing health conditions. Overall, promoting security awareness and implementing user-friendly privacy safeguards are essential for mHealth app utilization and data protection.

Despite regulations like GDPR and HIPAA, many free mHealth app users lack awareness of data processing, leaving apps vulnerable to breaches. Legal regulations may hinder medical app usage and are confusing to differentiate. Developing countries lack adequate digital health data protection laws. GDPR focuses on healthcare institutions, neglecting secure mHealth app construction and HIPAA guidelines mandate protection measures. GDPR ensures privacy protection with penalties, compensations, and user consent. Regular audits and law updates are advised, and non-compliant apps are barred from public deployment. Users should receive detailed privacy information before app usage, with informed consent emphasized for research or advertising purposes.

5. Limitation

This study, while offering fresh perspectives on privacy and confidentiality in mHealth app usage, is exploratory and comes with certain limitations. We acknowledge that relevant studies might have been overlooked if they were published in languages other than English, outside our specified time frame, or in databases not included in our search. Additionally, the chosen keywords for the search string may have excluded some studies. The varying privacy requirements of different types of apps suggest the importance of analyzing privacy concerns based on app type. Despite our efforts to address these limitations through expertise and detailed analysis, our categorization remains subjective. Given the absence of an existing classification system, this presents an opportunity for future research.

6. Conclusion

Based on the comprehensive review of privacy and confidentiality issues in mobile health (mHealth) applications, several key insights have emerged. mHealth applications have revolutionized healthcare by enhancing accessibility and ena-

bling better self-management of health, but they also present significant challenges regarding data privacy and security.

The study underscores the critical need for robust security frameworks during the development phase of mHealth applications. Effective integration of security measures such as encryption, multi-factor authentication, and secure data transfer protocols is essential to mitigate risks without compromising user experience. Additionally, clearly defined privacy policies are crucial for building user trust and ensuring transparency in data handling practices.

It is evident that educating users about the importance of security features and the implications of their consent is vital. Users must be made aware of privacy policies and the security measures in place to protect their data, thereby empowering them to make informed decisions about their health information.

Despite existing data protection methods and regulations like GDPR and HIPAA, many mHealth applications still fall short in compliance, leaving them vulnerable to breaches. Regular audits and updates to legal frameworks are necessary to keep pace with technological advancements and to maintain high standards of data security.

Future research should focus on developing a standardized classification system for privacy requirements tailored to different types of mHealth applications. This approach would help address the varying needs and risks associated with different app functionalities. Furthermore, exploring innovative technologies such as blockchain for decentralized and secure data storage could provide enhanced protection for sensitive health information.

In summary, while mHealth applications offer significant benefits, they also pose substantial privacy and security challenges. Addressing these challenges requires a multifaceted approach involving robust security frameworks, user education, regulatory compliance, and continuous innovation in data protection technologies. By tackling these issues, we can enhance the trust and effectiveness of mHealth applications in the global healthcare landscape.

Ethical Standards

This study received no specific grant from any funding agency.

Ethical Approval

This article does not contain any studies with animals performed by any of the authors.

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Dicianno, B.E., Parmanto, B., Fairman, A.D., Crytzer, T.M., Yu, D.X., Pramana, G.,

et al. (2015) Perspectives on the Evolution of Mobile (mHealth) Technologies and Application to Rehabilitation. *Physical Therapy*, **95**, 397-405. https://doi.org/10.2522/ptj.20130534

[2] Coiera, E. (2015) Guide to Health Informatics. 3rd Edition, CRC Press. https://doi.org/10.1201/b13617

[3] Larson, R.S. (2018) A Path to Better-Quality mHealth Apps. *JMIR mHealth and uHealth*, **6**, e10414. https://doi.org/10.2196/10414

[4] Nouri, R.R., Niakan Kalhori, S., Ghazisaeedi, M., Marchand, G. and Yasini, M. (2018) Criteria for Assessing the Quality of mHealth Apps: A Systematic Review. *Journal of the American Medical Informatics Association*, **25**, 1089-1098. https://doi.org/10.1093/jamia/ocy050

[5] Scott, K., Richards, D. and Adhikari, R. (2015) A Review and Comparative Analysis of Security Risks and Safety Measures of Mobile Health Apps. *Australasian Journal of Information Systems*, **19**, 1-18. https://doi.org/10.3127/ajis.v19i0.1210

[6] Cano, A.I.D. and Esplugues, A. (2023) Actualización y recomendación de apps sobre lactancia materna. *Anales De Pediatria*, **99**, 440-442.

[7] Roberts, A.E., Davenport, T.A., Wong, T., Moon, H., Hickie, I.B. and LaMonica, H.M. (2021) Evaluating the Quality and Safety of Health-Related Apps and E-Tools: Adapting the Mobile App Rating Scale and Developing a Quality Assurance Protocol. *Internet Interventions*, **24**, Article ID: 100379. https://doi.org/10.1016/j.invent.2021.100379

[8] Palos-Sanchez, P.R., Saura, J.R., Rios Martin, M.Á. and Aguayo-Camacho, M. (2021) Toward a Better Understanding of the Intention to Use mHealth Apps: Exploratory Study. *JMIR mHealth and uHealth*, **9**, e27021. https://doi.org/10.2196/27021

[9] Hussain, M., Al-Haiqi, A., Zaidan, A.A., Zaidan, B.B., Kiah, M., Iqbal, S., *et al.* (2018) A Security Framework for mHealth Apps on Android Platform. *Computers & Security*, **75**, 191-217. https://doi.org/10.1016/j.cose.2018.02.003

[10] Vo, V., Auroy, L. and Sarradon-Eck, A. (2019) Patients' Perceptions of mHealth Apps: Meta-Ethnographic Review of Qualitative Studies. *JMIR mHealth and uHealth*, **7**, e13817. https://doi.org/10.2196/13817

[11] Schroeder, T., Haug, M. and Gewald, H. (2022) Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study among Mature Adults. *JMIR Formative Research*, **6**, e28025. https://doi.org/10.2196/28025

[12] Sampat, B.H. and Prabhakar, B. (2017) Privacy Risks and Security Threats in mHealth Apps. *Journal of International Technology and Information Management*, **26**, 126-153. https://doi.org/10.58729/1941-6679.1353

[13] Manworren, N., Letwat, J. and Daily, O. (2016) Why You Should Care about the Target Data Breach. *Business Horizons*, **59**, 257-266. https://doi.org/10.1016/j.bushor.2016.01.002

[14] Khan, F., Kim, J.H., Mathiassen, L. and Moore, R. (2021) Data Breach Management: An Integrated Risk Model. *Information & Management*, **58**, Article ID: 103392. https://doi.org/10.1016/j.im.2020.103392

[15] Liu, L., Han, M., Wang, Y. and Zhou, Y. (2018) Understanding Data Breach: A Visualization Aspect. In: Chellappan, S., Cheng, W., Li, W., Eds., *Lecture Notes in Computer Science*, Springer, 883-892. https://doi.org/10.1007/978-3-319-94268-1_81

[16] Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E. and Carrasco, A. (2020) Privacy Assessment in Mobile Health Apps: Scoping Review. *JMIR*

mHealth and uHealth, **8**, e18868. https://doi.org/10.2196/18868

[17] Iwaya, L.H., Ahmad, A. and Babar, M.A. (2020) Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study. *IEEE Access*, **8**, 150081-150112. https://doi.org/10.1109/access.2020.3015962

[18] Chatzipavlou, I.A., Christoforidou, S.A. and Vlachopoulou, M. (2016) A Recommended Guideline for the Development of mHealth Apps. *mHealth*, **2**, 21-21. https://doi.org/10.21037/mhealth.2016.05.01

[19] Jusob, F.R., George, C. and Mapp, G. (2017) Exploring the Need for a Suitable Privacy Framework for mHealth When Managing Chronic Diseases. *Journal of Reliable Intelligent Environments*, **3**, 243-256. https://doi.org/10.1007/s40860-017-0049-7

[20] Rajput, A.R., Masood, I., Tabassam, A., Aslam, M.S., ShaoYu, Z. and Rajput, M.A. (2023) Patient's Data Privacy and Security in mHealth Applications: A Charles Proxy-Based Recommendation. *Soft Computing*, **27**, 18165-18180. https://doi.org/10.1007/s00500-023-09265-8

[21] Vithanwattana, N., Mapp, G. and George, C. (2017) Developing a Comprehensive Information Security Framework for mHealth: A Detailed Analysis. *Journal of Reliable Intelligent Environments*, **3**, 21-39. https://doi.org/10.1007/s40860-017-0038-x

[22] Yahya, F., Walters, R.J. and Wills, G.B. (2016) Goal-Based Security Components for Cloud Storage Security Framework: A Preliminary Study. 2016 *International Conference on Cyber Security and Protection of Digital Services* (*Cyber Security*), London, 13-14 June 2016, 1-5. https://doi.org/10.1109/cybersecpods.2016.7502338

[23] Thamilarasu, G. and Lakin, C. (2017) A Security Framework for Mobile Health Applications. 2017 5*th International Conference on Future Internet of Things and Cloud Workshops* (*FiCloudW*), Prague, 21-23 August 2017, 221-226. https://doi.org/10.1109/ficloudw.2017.96

[24] Srivastava, M. and Thamilarasu, G. (2019) MSF: A Comprehensive Security Framework for mHealth Applications. 2019 7*th International Conference on Future Internet of Things and Cloud Workshops* (*FiCloudW*), Istanbul, 26-28 August 2019, 70-75. https://doi.org/10.1109/ficloudw.2019.00026

[25] Jusob, F.R., George, C. and Mapp, G. (2021) A New Privacy Framework for the Management of Chronic Diseases via mHealth in a Post-Covid-19 World. *Journal of Public Health*, **30**, 37-47. https://doi.org/10.1007/s10389-021-01608-9

[26] Saracevic, M.H., Adamovic, S.Z., Miskovic, V.A., Elhoseny, M., Macek, N.D., Selim, M.M., *et al.* (2021) Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. *IEEE Transactions on Reliability*, **70**, 819-830. https://doi.org/10.1109/tr.2020.3010973

[27] Galvin, H.K. and DeMuro, P.R. (2020) Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019. *Yearbook of Medical Informatics*, **29**, 32-43. https://doi.org/10.1055/s-0040-1701987

[28] Ahmad, G.I., Singla, J. and Giri, K. J. (2021) Security and Privacy of E-Health Data. In: Giri, K.J., Parah, S.A., Bashir, R. and Muhammad, K., Eds., *Multimedia Security: Algorithm Development, Analysis and Applications*, Springer, 199-214. https://doi.org/10.1007/978-981-15-8711-5_10

[29] Zhou, P., Zhou, G., Wu, D. and Fei, M. (2021) Detecting Multi-Stage Attacks Using Sequence-to-Sequence Model. *Computers & Security*, **105**, Article ID: 102203. https://doi.org/10.1016/j.cose.2021.102203

[30] Morera, E.P., de la Torre Díez, I., Garcia-Zapirain, B., López-Coronado, M. and

Arambarri, J. (2016) Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide. *Journal of Medical Systems*, **40**, Article No. 152. https://doi.org/10.1007/s10916-016-0513-6

[31] Martínez-Pérez, B., de la Torre-Díez, I. and López-Coronado, M. (2014) Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, **39**, Article No. 181. https://doi.org/10.1007/s10916-014-0181-3

[32] Shafique, U., Khan, H., Waqar, S., Sher, A., Zeb, A., Shafi, U., *et al.* (2017) Modern Authentication Techniques in Smart Phones: Security and Usability Perspective. *International Journal of Advanced Computer Science and Applications*, **8**, 331-340. https://doi.org/10.14569/ijacsa.2017.080142

[33] Kharrazi, H., Chisholm, R., Van Nasdale, D. and Thompson, B. (2012) Mobile Personal Health Records: An Evaluation of Features and Functionality. *International Journal of Medical Informatics*, **81**, 579-593. https://doi.org/10.1016/j.ijmedinf.2012.04.007

[34] Mustafa, U., Pflugel, E. and Philip, N. (2019) A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. 2019 *IEEE* 12*th International Conference on Global Security*, *Safety and Sustainability* (*ICGS*3), London, 16-18 January 2019, 1-9. https://doi.org/10.1109/icgs3.2019.8688019

[35] Hasan, M.K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.A., Habib, S., *et al.* (2021) Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. *IEEE Access*, **9**, 47731-47742. https://doi.org/10.1109/access.2021.3061710

[36] Tan, S., Lo, K.C., Leau, Y., Chung, G. and Ahmedy, F. (2021) Securing mHealth Applications with Grid-Based Honey Encryption. 2021 *IEEE International Conference on Artificial Intelligence in Engineering and Technology* (*IICAIET*), Kota Kinabalu, 13-15 September 2021, 1-5. https://doi.org/10.1109/iicaiet51634.2021.9573645

[37] Deebak, B.D., Al-Turjman, F., Aloqaily, M. and Alfandi, O. (2019) An Authentic-Based Privacy Preservation Protocol for Smart E-Healthcare Systems in IoT. *IEEE Access*, **7**, 135632-135649. https://doi.org/10.1109/access.2019.2941575

[38] Zhou, L. and Parmanto, B. (2020) User Preferences for Privacy Protection Methods in Mobile Health Apps: A Mixed-Methods Study. *International Journal of Telerehabilitation*, **12**, 13-26. https://doi.org/10.5195/ijt.2020.6319

[39] Enamamu, T., Otebolaku, A., Marchang, J. and Dany, J. (2020) Continuous M-Health Data Authentication Using Wavelet Decomposition for Feature Extraction. *Sensors*, **20**, Article 5690. https://doi.org/10.3390/s20195690

[40] Huh, J. (2020) Surgery Agreement Signature Authentication System for Mobile Health Care. *Electronics*, **9**, Article 890. https://doi.org/10.3390/electronics9060890

[41] Egala, B.S., Pradhan, A.K., Badarla, V. and Mohanty, S.P. (2021) Fortified-chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. *IEEE Internet of Things Journal*, **8**, 11717-11731. https://doi.org/10.1109/jiot.2021.3058946

[42] Thabit, R. (2019) Review of Cryptography Applications in eHealth Security Systems. *International Journal of Science and Engineering Investigations*, **8**, 110-116.

[43] van Haasteren, A., Gille, F., Fadda, M. and Vayena, E. (2019) Development of the mHealth App Trustworthiness Checklist. *Digital Health*, **5**. https://doi.org/10.1177/2055207619886463

[44] Mia, M.R., Shahriar, H., Valero, M., Sakib, N., Saha, B., Barek, M.A., *et al.* (2022) A Comparative Study on HIPAA Technical Safeguards Assessment of Android

mHealth Applications. *Smart Health*, **26**, Article ID: 100349. https://doi.org/10.1016/j.smhl.2022.100349

[45] Braghin, C., Cimato, S. and Della Libera, A. (2018) Are mHealth Apps Secure? A Case Study. 2018 *IEEE* 42*nd Annual Computer Software and Applications Conference* (*COMPSAC*), Tokyo, 23-27 July 2018, 335-340. https://doi.org/10.1109/compsac.2018.10253

[46] Nagaraj, S., Raju, G.S.V.P. and Srinadth, V. (2015) Data Encryption and Authetication Using Public Key Approach. *Procedia Computer Science*, **48**, 126-132. https://doi.org/10.1016/j.procs.2015.04.161

[47] Shuwandy, M.L., Zaidan, B.B., Zaidan, A.A., Albahri, A.S., Alamoodi, A.H., Albahri, O.S., *et al.* (2020) mHealth Authentication Approach Based 3D Touchscreen and Microphone Sensors for Real-Time Remote Healthcare Monitoring System: Comprehensive Review, Open Issues and Methodological Aspects. *Computer Science Review*, **38**, Article ID: 100300. https://doi.org/10.1016/j.cosrev.2020.100300

[48] Jaeger, J., Ristenpart, T. and Tang, Q. (2016) Honey Encryption Beyond Message Recovery Security. In: Fischlin, M. and Coron, J.S., Eds., *Lecture Notes in Computer Science*, Springer, 758-788. https://doi.org/10.1007/978-3-662-49890-3_29

[49] Daley, B.J., Ni'Man, M., Neves, M.R., Bobby Huda, M.S., Marsh, W., Fenton, N.E., *et al.* (2021) mHealth Apps for Gestational Diabetes Mellitus That Provide Clinical Decision Support or Artificial Intelligence: A Scoping Review. *Diabetic Medicine*, **39**, e14735. https://doi.org/10.1111/dme.14735

[50] Silva, B.M., Rodrigues, J.J., Canelo, F., Lopes, I.C. and Zhou, L. (2013) A Data Encryption Solution for Mobile Health Apps in Cooperation Environments. *Journal of Medical Internet Research*, **15**, e66. https://doi.org/10.2196/jmir.2498

[51] Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S.D., Yan, X., *et al.* (2021) Privacy Paradox in mHealth Applications: An Integrated Elaboration Likelihood Model Incorporating Privacy Calculus and Privacy Fatigue. *Telematics and Informatics*, **61**, Article ID: 101601. https://doi.org/10.1016/j.tele.2021.101601

[52] O'Loughlin, K., Neary, M., Adkins, E.C. and Schueller, S.M. (2019) Reviewing the Data Security and Privacy Policies of Mobile Apps for Depression. *Internet Interventions*, **15**, 110-115. https://doi.org/10.1016/j.invent.2018.12.001

[53] Parker, L., Halter, V., Karliychuk, T. and Grundy, Q. (2019) How Private Is Your Mental Health App Data? An Empirical Study of Mental Health App Privacy Policies and Practices. *International Journal of Law and Psychiatry*, **64**, 198-204. https://doi.org/10.1016/j.ijlp.2019.04.002

[54] Robillard, J.M., Feng, T.L., Sporn, A.B., Lai, J., Lo, C., Ta, M., *et al.* (2019) Availability, Readability, and Content of Privacy Policies and Terms of Agreements of Mental Health Apps. *Internet Interventions*, **17**, Article ID: 100243. https://doi.org/10.1016/j.invent.2019.100243

[55] Zhou, L., Bao, J., Watzlaf, V. and Parmanto, B. (2019) Barriers to and Facilitators of the Use of Mobile Health Apps from a Security Perspective: Mixed-Methods Study. *JMIR mHealth and uHealth*, **7**, e11223. https://doi.org/10.2196/11223

[56] Sardi, L., Idri, A., Redman, L.M., Alami, H., Bezad, R. and Fernández-Alemán, J.L. (2020) Mobile Health Applications for Postnatal Care: Review and Analysis of Functionalities and Technical Features. *Computer Methods and Programs in Biomedicine*, **184**, Article ID: 105114. https://doi.org/10.1016/j.cmpb.2019.105114

[57] Sunyaev, A., Dehling, T., Taylor, P.L. and Mandl, K.D. (2014) Availability and Quality of Mobile Health App Privacy Policies. *Journal of the American Medical Informatics Association*, **22**, e28-e33. https://doi.org/10.1136/amiajnl-2013-002605

[58] Shipp, L. and Blasco, J. (2020) How Private Is Your Period? A Systematic Analysis of Menstrual App Privacy Policies. *Proceedings on Privacy Enhancing Technologies*, **2020**, 491-510. https://doi.org/10.2478/popets-2020-0083

[59] Amanul Islam, M. (2022) Privacy Risks and Security Threat Strategy to Optimize the Vulnerability in Health Information System (HIS). *International Journal of Advanced Networking and Applications*, **14**, 5271-5276. https://doi.org/10.35444/ijana.2022.14106

[60] He, D., Naveed, M., Gunter, C.A. and Nahrstedt, K. (2014) Security Concerns in Android mHealth Apps. *AMIA Annual Symposium Proceedings*, **2014**, 645–654.

[61] Greene, E., Proctor, P. and Kotz, D. (2019) Secure Sharing of mHealth Data Streams through Cryptographically-Enforced Access Control. *Smart Health*, **12**, 49-65. https://doi.org/10.1016/j.smhl.2018.01.003

[62] Ammar, N., Bailey, J.E., Davis, R.L. and Shaban-Nejad, A. (2021) Using a Personal Health Library-Enabled mHealth Recommender System for Self-Management of Diabetes among Underserved Populations: Use Case for Knowledge Graphs and Linked Data. *JMIR Formative Research*, **5**, e24738. https://doi.org/10.2196/24738

[63] Cvrkel, T. (2018) The Ethics of mHealth: Moving Forward. *Journal of Dentistry*, **74**, S15-S20. https://doi.org/10.1016/j.jdent.2018.04.024

[64] Gurupur, V.P. and Wan, T.T.H. (2017) Challenges in Implementing mHealth Interventions: A Technical Perspective. *mHealth*, **3**, Article 32. https://doi.org/10.21037/mhealth.2017.07.05

[65] Hathaliya, J.J. and Tanwar, S. (2020) An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0. *Computer Communications*, **153**, 311-335. https://doi.org/10.1016/j.comcom.2020.02.018

[66] Ren, Y., Shen, J., Zheng, Y., Wang, J. and Chao, H. (2015) Efficient Data Integrity Auditing for Storage Security in Mobile Health Cloud. *Peer-to-Peer Networking and Applications*, **9**, 854-863. https://doi.org/10.1007/s12083-015-0346-y

[67] Benaloh, J., Chase, M., Horvitz, E. and Lauter, K. (2009) Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. *Proceedings of the* 2009 *ACM Workshop on Cloud Computing Security*, Chicago, 13 November 2009, 103-114. https://doi.org/10.1145/1655008.1655024

[68] Aljedaani, B., Ahmad, A., Zahedi, M. and Babar, M.A. (2023) End-Users' Knowledge and Perception about Security of Clinical Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers. *Journal of Systems and Software*, **195**, Article ID: 111519. https://doi.org/10.1016/j.jss.2022.111519

[69] Plachkinova, M., Andres, S. and Chatterjee, S. (2015) A Taxonomy of mHealth Apps—Security and Privacy Concerns. 2015 48*th Hawaii International Conference on System Sciences*, Kauai, 5-8 January 2015, 3187-3196. https://doi.org/10.1109/hicss.2015.385

[70] Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F.N., Al-Mugheed, K., Anshasi, R.J., *et al.* (2023) The Use of a Technology Acceptance Model (TAM) to Predict Patients' Usage of a Personal Health Record System: The Role of Security, Privacy, and Usability. *International Journal of Environmental Research and Public Health*, **20**, Article 1347. https://doi.org/10.3390/ijerph20021347

[71] Yarbrough, A.K. and Smith, T.B. (2007) Technology Acceptance among Physicians: A New Take on TAM. *Medical Care Research and Review*, **64**, 650-672. https://doi.org/10.1177/1077558707305942

[72] Aydin, G. (2023) Increasing Mobile Health Application Usage among Generation Z Members: Evidence from the UTAUT Model. *International Journal of Pharmaceu-*

tical and Healthcare Marketing, **17**, 353-379.
https://doi.org/10.1108/ijphm-02-2021-0030

[73] Shemesh, T. and Barnoy, S. (2020) Assessment of the Intention to Use Mobile Health Applications Using a Technology Acceptance Model in an Israeli Adult Population. *Telemedicine and e-Health*, **26**, 1141-1149.
https://doi.org/10.1089/tmj.2019.0144

[74] Hilty, D.M., Chan, S., Torous, J., Luo, J. and Boland, R.J. (2019) A Telehealth Framework for Mobile Health, Smartphones, and Apps: Competencies, Training, and Faculty Development. *Journal of Technology in Behavioral Science*, **4**, 106-123.
https://doi.org/10.1007/s41347-019-00091-0

[75] Boyles, J.L., Smith, A. and Madden, M. (2012) Privacy and Data Management on Mobile Devices. *Pew Internet & American Life Project*, **4**, 1-19.

[76] Mancini, E. (2023) Privacy and Security Analysis of mHealth Apps.
https://thesis.unipd.it/handle/20.500.12608/46196

[77] Sheppard, M.K. (2020) mHealth Apps: Disruptive Innovation, Regulation, and Trust—A Need for Balance. *Medical Law Review*, **28**, 549-572.
https://doi.org/10.1093/medlaw/fwaa019

[78] Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B. (2018) Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society*, **39**, 283-297. https://doi.org/10.1016/j.scs.2018.02.014

[79] Shu, I.N. and Jahankhani, H. (2017) The Impact of the New European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England. 2017 *Cybersecurity and Cyberforensics Conference* (*CCC*), London, 21-23 November 2017, 31-37. https://doi.org/10.1109/ccc.2017.16

[80] Oliva, A., Grassi, S., Vetrugno, G., Rossi, R., Della Morte, G., Pinchi, V., *et al.* (2022) Management of Medico-Legal Risks in Digital Health Era: A Scoping Review. *Frontiers in Medicine*, **8**, Article 821756. https://doi.org/10.3389/fmed.2021.821756

[81] Jain, D. (2023) Regulation of Digital Healthcare in India: Ethical and Legal Challenges. *Healthcare*, **11**, Article 911. https://doi.org/10.3390/healthcare11060911

[82] Knorr, K. and Aspinall, D. (2015) Security Testing for Android mHealth Apps. 2015 *IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops* (*ICSTW*), Graz, 13-17 April 2015, 1-8.
https://doi.org/10.1109/icstw.2015.7107459

[83] Kotz, D., Gunter, C.A., Kumar, S. and Weiner, J.P. (2016) Privacy and Security in Mobile Health: A Research Agenda. *Computer*, **49**, 22-30.
https://doi.org/10.1109/mc.2016.185

[84] Ducato, R. (2016) Cloud Computing for S-Health and the Data Protection Challenge: Getting Ready for the General Data Protection Regulation. 2016 *IEEE International Smart Cities Conference* (*ISC*2), Trento, 12-15 September 2016, 1-4.
https://doi.org/10.1109/isc2.2016.7580803

[85] Hendricks-Sturrup, R. (2022) Pulse Oximeter App Privacy Policies during COVID-19: Scoping Assessment. *JMIR mHealth and uHealth*, **10**, e30361.
https://doi.org/10.2196/30361

[86] Nurgalieva, L., O'Callaghan, D. and Doherty, G. (2020) Security and Privacy of mHealth Applications: A Scoping Review. *IEEE Access*, **8**, 104247-104268.
https://doi.org/10.1109/access.2020.2999934

[87] Tung, B. (2021) The Challenges of Applying Computational Legal Analysis to mHealth Security and Privacy Regulations. Master's Thesis, McKelvey School of Engineering.

[88] Tangari, G., Ikram, M., Ijaz, K., Kaafar, M.A. and Berkovsky, S. (2021) Mobile Health and Privacy: Cross Sectional Study. *BMJ*, **373**, n1248. https://doi.org/10.1136/bmj.n1248