ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 2, pp. 355-371
DOI:10.33168/JSMS.2024.0222

Security and Privacy Policy Assessment in Mobile Health Applications: A Literature Review

Nashrul Hakiem [1], Sandra Hakiem Afrizal [2], Yudi Setiadi [3], Hadid Syaifullah Albab [1], Mardhani Riasetiawan [4], Sonny Zulhuda [5]

[1]Faculty of Science and Technology, Universitas Islam Negeri Syarif Hidayatullah, Jakarta, Indonesia
[2]Faculty of Health Sciences and Technology, Universitas Binawan, Jakarta, Indonesia
[3]Internal Control Audit, Universitas Islam Negeri Syarif Hidayatullah, Jakarta, Indonesia
[4]Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Yogyakarta, Indonesia
[5]Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia
hakiem@uinjkt.ac.id

Abstract. Currently, the availability of mobile health (mHealth) applications is growing, implying the development and effectiveness of healthcare facilities. However, the sensitive medical information potentially intrudes into the privacy and security of users which has not been acknowledged by the user. The lack of guidance regarding privacy policy assessment causes concern with the development of privacy policy requirements based on privacy and security dimensions. This study objectives to identify the requirements of the privacy policy in mHealth applications. A narrative review has been conducted using keywords to find related open-source literature published from 2015 to 2022 from Science Direct, PMC, and PubMed databases to identify the privacy and security assessments based on the perspective of mHealth App research. A total of 17 articles were reviewed using the keywords “privacy policy” AND “privacy” AND “security” AND “mobile health”. Three major requirements were found related to privacy and security frameworks namely consistency and transparency, data management and processing, and interconnected-data arrangement. Consistency and transparency involve clear processes, data types, legal safeguards, access provisions, data sharing transparency, and data quality maintenance. Data management and processing require disclosure mechanisms, robust technical security measures, and protocols for vulnerable users. Lastly, an interconnected data arrangement should include data arrangement identification, data sharing policies, and data interconnection procedures.

Keywords: privacy policy, privacy and security assessment, mobile health Apps, digital health

1. Introduction

The COVID-19 pandemic has triggered a heightened adoption of digital health solutions within society. Digital health, which includes mobile health or mHealth, leverages technology like telemedicine, surveillance, education, health monitoring, and decision support to revolutionise the healthcare sector (Elliot Mbunge et al., 2022). The use of mHealth often involves data transfer facilitated by communication technologies on smartphones, encompassing contact information, location, and media galleries (Yang et al., 2013). The implementation of smartphone Apps and wearable sensors for clinical assessments, symptom tracking, and treatment can potentially expose patient data to external entities (Hussain et al., 2018). However, the transmission of data through these applications may also jeopardize user privacy and security (Morera et al., 2016).

Security refers to the set of procedural and technical actions necessary to deter unauthorised entry, alteration, utilization, and distribution of data stored or managed within a computer system, with the intention of safeguarding the system from physical damage (Centers for Medicare and Medicaid Services, 2021). Meanwhile, privacy primarily focuses on the acquisition, retention, and utilization of personal data, as well as the feasibility of gathering data and its subsequent utilization by external entities (Nass et al., 2009). While technical mechanisms like encryption are crucial for data security, evaluating privacy policies is also essential to ensure transparency and compliance with regulations. Therefore, this review specifically concentrates on the frameworks and criteria utilised to assess privacy policies in mHealth apps within the literature. Moreover, the primary objective of security and privacy revolves around effectively safeguarding individuals' health information, all the while facilitating the necessary exchange of data essential for advancing superior healthcare services. However, the rise of cases of personal data theft shows that there are challenges related to security and privacy in various sectors including the health sector.

The lack of privacy and security aspect compliance when designing a mobile health application may increase the possibility of malware attacks (Lagan et al., 2021). From the security aspect, user data encryption, secure internet connection, and security features such as strong passwords, protection for several surfaces such as Bluetooth, and SD card storage can potentially increase data security. Regarding privacy considerations, mHealth Applications on Google Play often transmit sensitive medical information as plain text and store it on third-party servers, lacking appropriate confidentiality and privacy protocols for handling this specific data type (Hussain et al., 2018). According to a recent study, mobile health Apps frequently transmit private user data to unknown destinations without the consent of the user (Xu et al., 2018). A previous study also found that certain smartphone Apps may not respect the privacy of personal health information and may be able to collect or sell the data (Lagan et al., 2021). Figure 1 shows that third-party libraries such as Google Ads for advertisements and Google Analytics for analytics were identified within the code and files of 45.3% (3659) of medical apps and nearly 50.0% (6453) of health and fitness apps, as reported by (Tangari et al., 2021).

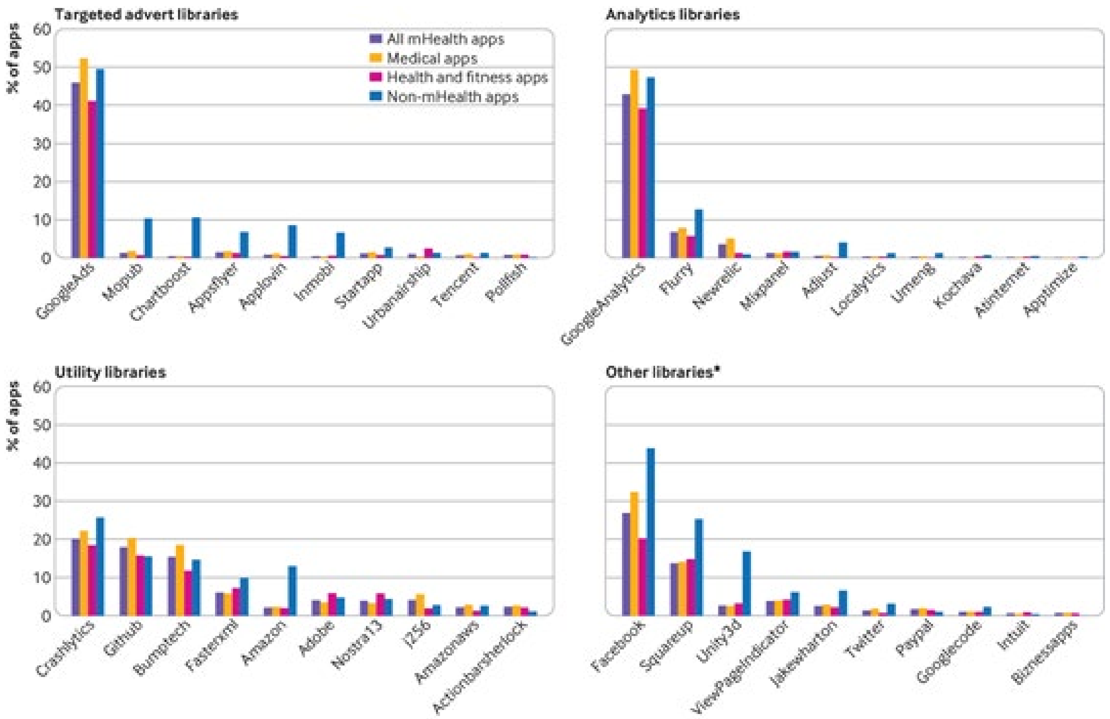

Fig. 1. Third party libraries in mHealth app categories and non-mHealth apps (Tangari et al., 2021)

Compliance with privacy regulations is the legal aspect to regulate user data management and to avoid the misuse of the data. To assist compliance with the privacy regulations for mHealth technology implementation, federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), have been enacted to establish nationwide benchmarks aimed at safeguarding the medical records of individuals and various other aspects of individual health information within the United States (Proposed Rule Standards for Privacy of Individually Identifiable Health Information, 1999). However, the regulations may not apply to entities that collect health information from mobile Apps or sensors concerning what extent shared data should be anonymised or the impact of sharing such data on user privacy. A recent study found that most of the articles concerning health technology with regard to patient information of healthcare did not report the participant's perception of privacy (Cornet & Holden, 2018). Related to the research, the understanding of each patient through consent should be obtained when using data from digital health technologies such as what personal information is collected, how often the data is collected, to what parties the information is disclosed, etc. (Dinh-Le et al., 2019).

The establishment of clear and consistent privacy policy standards would significantly improve the efficiency and effectiveness of the healthcare system. Nevertheless, the absence of tools to assist users and practitioners in selecting secure and efficient mobile health (mHealth) applications has resulted in an increasing risk of health information misuse due to users' limited awareness of the importance of privacy and security. A study conducted by (Pang et al., 2020) identified nine distinct categories of privacy concerns, including access, consent, design, governance, legal, risk, security, social, and trust. Their research revealed that mHealth users are particularly concerned about the potential leakage and misuse of their data. However, there is a notable gap in research regarding the legal aspects of privacy and security. Hence, this study aims to explore and identify privacy and security requirements through an analysis of the privacy policies of mobile health applications, drawing upon established security and privacy frameworks.

2. Literature Study

2.1. Security and Privacy Regulations and Frameworks

The security regulations are designed to be flexible and scalable to assist the implementation of new technology for improving healthcare. The Federal law the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the United States is one of the established standards and safeguards for maintaining health information through privacy and security regulations. HIPAA covers entities such as health information transmission through electronic forms, health plans, healthcare clearinghouses, and business associates (Centers for Medicare and Medicaid Services, 2021). Offering further context, the General Data Protection Regulation (GDPR), implemented by the European Union in 2018, has revolutionised data protection globally. It addresses the collection, processing, and storage of personal data, ensuring the privacy and security of individuals' information (Benjumea et al., 2020; Hatamian et al., 2021). Due to the regulations, health systems should ensure that health information management systems through technology may be considered as a secure network as they may be monitored continuously.

Table 1 Security and Privacy Objectives (National Institute of Standards and Technology, 2020)

Topic	Objective	Definition
Privacy	Predictability	This refers to the capability of enabling individuals, owners, and operators to make reliable assumptions about data and its processing within a system.
	Manageability	It involves the facilitation of comprehensive data administration, which includes tasks such as data collection, modification, deletion, and selective disclosure.
	Disassociability	This characteristic enables the independent processing of data or events, ensuring that they are not connected to particular individuals or devices beyond what is essential for the system's operational needs.
Security	Confidentiality	This aspect focuses on maintaining authorised limitations on accessing and revealing information, guaranteeing the safeguarding of personal privacy and proprietary data.
	Integrity	This encompasses safeguarding data against unauthorised modifications or destruction, including measures to ensure the non-repudiation and authenticity of information.
	Availability	This aspect ensures that information is timely, accessible, and available for utilization as needed.

Following HIPAA requirements, many protection practices have been studied to secure patient information such as frequent monitoring or studies related to security techniques including a firewall to block unauthorised connections either from internal or external connections and cryptography which involves the use of digital signatures and usernames or passwords (Proposed Rule Standards for Privacy of Individually Identifiable Health Information, 1999)(National Institute of Standards and Technology, 2017). Certain cryptographic mechanisms, utilizing both symmetric and asymmetric encryption (Rudnytskyi et al., 2022), as well as network security, have been improved through the use of contemporary technologies, including Artificial Intelligence (Liu & Zhang, 2023). An additional option to secure health information includes the separation of patient health data that cannot be accessed through the Internet to prevent malware from infiltrating the network connection and setting policies to prevent users from downloading external software through the Internet.

Numerous privacy assessment frameworks and tools have been employed. For example, in some research, the Integrated Safety, Security, and Privacy (ISSP) Risk Assessment Framework (Yaqoob et al., 2020) was suggested to gauge device risk levels and prescribe necessary security measures. Moreover, a conceptual threat assessment framework has been introduced for enhancing the security of Consumer Health Wearables (Mnjama et al., 2017). The National Institute of Standard Technology or NIST added a privacy framework to ISO 27001 for information security which is useful in managing security and privacy requirements as illustrated in Table 1.

2.2. Security and Privacy of mHealth Applications

In the present times of the COVID-19 pandemic, digital technologies could improve access to healthcare. For example, telemedicine may be used which provides healthcare from a distance using technology such as video conferencing and interactive texting (Shore et al., 2018)(Elliot Mbunge et al., 2022). The clinicians and patients could have the possibility to protect their health information data through a closed discussion. However, the lack of protection of personal health information has caused unauthorised access to take place to personalised health records. Previous research has found that more than 100 million records were exposed by an unauthorised body (Nurgalieva et al., 2020).

Protection of mobile health information consists of three areas of concern includes network security, the use of equipment in an outside area and patients using public spaces during the care session, and app evaluation (Ruotsalainen & Blobel, 2020). Network security recommendations include encryption of video or audio transmissions, authentication features for security, updated antivirus, and firewall software (Shore et al., 2018). While other recommendations released by the American Psychiatric Association (APA) which has a 5 step App evaluation model as follows (American Psychiatric Association, 2022): 1) Access and background to ensure the background information about the App are appropriate to be evaluated by the user, 2) privacy and safety to help the user to consider the aspect of privacy and security, 3) clinical foundation to evaluate any evidence for health benefits, 4) usability to recap the usefulness of the App in terms of functionality, and 5) data integration towards a therapeutic goal as the top level of how to share the data after passing the previous steps and deciding to use the App.

3. Research Methods

The search for relevant papers published between 2015 and 2022 involved a literature search utilizing specific keywords, including: “privacy policy” AND “privacy” AND “security” AND “mobile health”. The inclusion criteria were limited to articles published in English and presented either as conference papers or regular articles.

The following steps of the literature search process are described in Figure 2. The search process began by identifying the appropriate keywords for searching relevant articles. Subsequently, the selection of PubMed, ScienceDirect, and PMC was based on their established reputations as reliable sources of academic research. These databases were chosen for their comprehensive coverage of medical, multidisciplinary, and biomedical literature, ensuring access to relevant studies related to mHealth app privacy policies. Once the keywords were applied, the authors proceeded to select the articles while eliminating any duplicate entries. The final step involved reviewing all the selected articles and excluding any that did not align with the study's objectives.

3.1. Scope and research strategy

The primary focus of this research centers around two key domains: (1) security and privacy requirements, and (2) the scope of mHealth applications. To address these areas, the study has been structured into three research questions:

1. What are the specific privacy and security concerns that have been identified in mHealth Apps?
2. What evaluation techniques have been employed to evaluate the privacy and security aspects of mHealth Apps?
3. What are the pre-existing requirements that have been identified before conducting the assessment?

3.2. Empirical phase

The research design involved an empirical phase aimed at gaining insights into the research area of interest. This was achieved through a systematic mapping of literature works, which facilitated the identification of trends in the topic. The data collection process was well-defined and comprised four stages: preparation, conduction, elimination, and reporting.

During the preparation stage, the main goal, research questions, relevant keywords, database identification, and inclusion and exclusion criteria were established. The process started with the application of keywords through the databases, followed by the screening of articles grounded in the predetermined criteria of inclusion and exclusion. All identified articles were assessed for relevance based on their titles and abstracts. Subsequently, two authors independently reviewed the full texts of the selected articles to determine if they met the inclusion criteria. Any discrepancies between the two authors were resolved through discussion among the team. Finally summarising and analysing of the selected papers based on the research questions (see Figure 2).

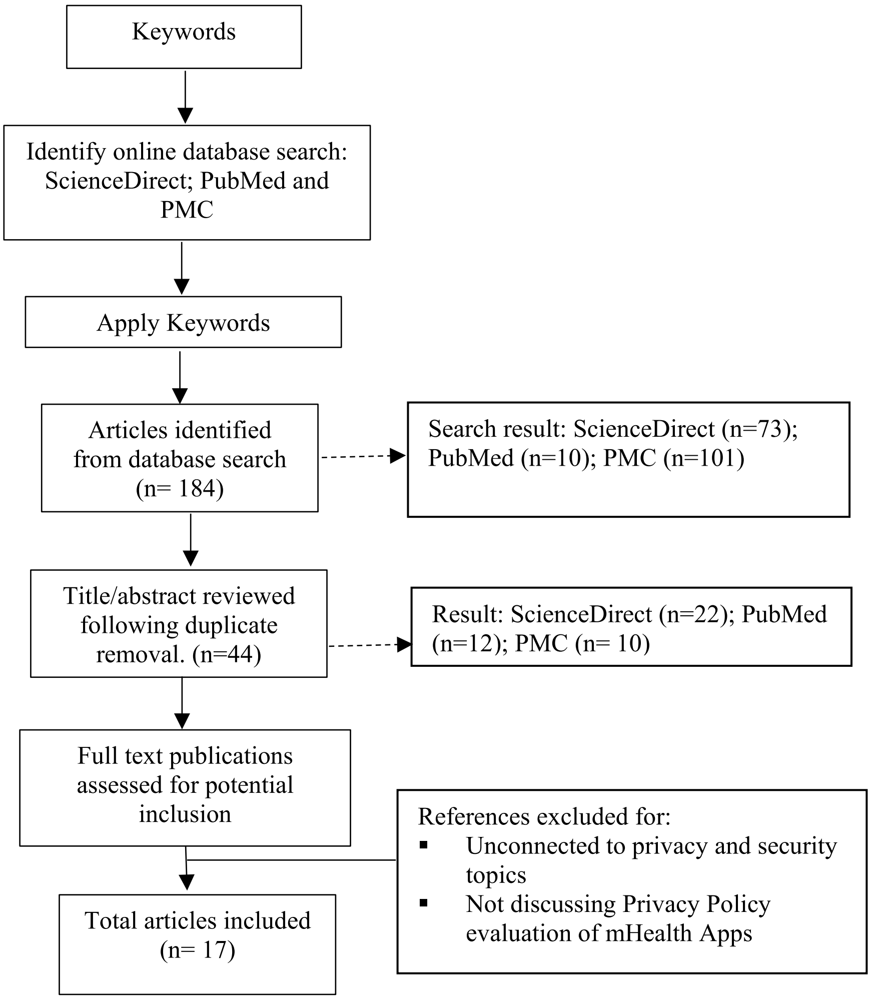
Keywords
Identify online database search: ScienceDirect; PubMed and PMC
Apply Keywords
Articles identified from database search (n= 184)
Search result: ScienceDirect (n=73); PubMed (n=10); PMC (n=101)
Title/abstract reviewed following duplicate removal. (n=44)
Result: ScienceDirect (n=22); PubMed (n=12); PMC (n= 10)
Full text publications assessed for potential inclusion
References excluded for:
Unconnected to privacy and security topics
Not discussing Privacy Policy evaluation of mHealth Apps
Total articles included (n= 17)

Fig. 2. Literature search steps

3.3. Mobile App Privacy Policy Assessment

To meet the security and privacy goals of stakeholders or users, a system, product, or service must adhere to specific criteria in terms of data elements, content, design, and functionality. The privacy and security objectives, as outlined by NIST (National Institute of Standards and Technology), encompass three main objectives for privacy assessment which is predictability through consistency and transparency aspects, manageability through data management and processing aspect, and disassociability through an interconnected-data arrangement.

4. Results

4.1. Data Collection and Scope

A total of 17 articles concerning mHealth privacy and security assessment were reviewed. It was found that 5 articles examined security and privacy in mental health Apps, while 2 articles assessed chronic disease Apps. The other articles reviewed cancer Apps (2 articles), Covid-19 Apps (1 article), women's health Apps (2 articles), and mHealth in general (5 articles). Detailed information such as the scope of Apps, methods used, and evaluation framework for App characteristics are explained in Table 2.

Table 2. The empirical phase of the review

No	Source	Scope of App	The research aims and method	Security and Privacy Requirements
1	(Hatamian et al., 2021)	COVID-19 Apps using Android and iOS	A systematic analysis of privacy and security performance based on features and functions of COVID-19 mobile Apps.	The privacy policy analysis is solely based on the GDPR such as Data Collection, children protection, 3rd party sharing, 3rd country sharing, data protection, data retention, user control, privacy policy changes, privacy breach notice, app-focused, purpose specification, contact information
2	(Huckvale et al., 2019)	Evaluation of Mobile Applications for Addressing Depression and Smoking Cessation on Android and iOS Platforms.	Cross-sectional evaluation of the privacy policy.	Employing criteria to assess the quality of privacy policies, encompassing primary and secondary data usage, data transmission, subject access rights, technical security measures, governance, and operational controls.
3	(Tangari et al., 2021)	Applications related to medical and health fitness sectors.	A cross-sectional study to investigate and define the privacy procedures of mHealth Applications available on Google Play.	App privacy was characterised through 3rd party presence, data collection operations such as permission to gain entry to elements of the operating system (location, contact, etc.), privacy policy analysis, traffic analysis, advertisements and trackers, personal data transmission in application data flow, safeguarded transmission of user information such as using Hypertext Transfer Protocol Secure or HTTPS to protect the user's privacy, and App review analysis.
4	(Sunyaev et al., 2015)	mHealth Apps in iOS and Android.	A cross-sectional study to identify the accessibility, range, and clarity of health Applications.	The availability of a privacy policy was assessed and counted while a transparency policy was determined by the nature of gathered data (sensitive or not), reasons behind data collection (App functionality, data utilization), dissemination of data (third-party involvement), and user oversight (monitoring, alerts).
5	(Parker et al., 2019)	Mental health Apps	A mixed-method study to identify privacy-related problems amongst mental health App users by applying a thorough examination of privacy-oriented details.	The availability of privacy policy was confirmed through practices i.e.: App requests for data collection or permission, promoting the value of sharing. The availability of privacy policies such as policy accessibility and readability.
6	(Bookert et al., 2022)	Internet of Medical Things (IoMT) devices in smart homes	Privacy policy text evaluation from 20 IoMT devices using Privacy Policy Assessment Questionnaire	Seven privacy considerations: age limitations, information collection, information sharing, data storage duration, data safeguarding, user preferences, and protection of children's personal data.

No	Source	Scope of App	The research aims and method	Security and Privacy Requirements
7	(Benjumea et al., 2020)	Breast Cancer mHealth Apps.	privacy policy assessment using a systematic search	General Data Protection Regulation (GDPR) framework has been used through 14 items of the privacy checklist such as the identity of the entity responsible for data control, identity of the representative, particulars of the data protection officer, processing objectives, legal foundation for processing, legitimate interests of the controller, recipients (or groups) of personal data, duration of data retention, acknowledgment of data subject rights, right to retract consent, ability to file grievances with a regulatory body, necessity to provide personal information, presence of automated decision-making, and implementation of profiling.
8	(Minen et al., 2018)	Headache/Migraine Applications.	The examination of privacy policies in headache and migraine Apps.	The examination was classified into: data storage explanation such as local on the user's devices or external, permitting sharing with third parties, data storage, third parties, underage regulation, and granted user data.
9	(Hendricks-Sturrup, 2022)	Pulse oximeter Apps.	Evaluation of privacy policy in oximeter Apps.	The assessment was carried out by examining an accessible privacy policy, focusing on details related to the privacy policy. These included information such as the developer's location (country), whether the App is free or requires payment for use/subscription, the presence of ads disclosure on the App's site, the extent of personal data collection, considerations of proportionality, fundamental rights, data protection, and privacy concerns, as well as the implementation of privacy safeguards.
10	(Alfawzan et al., 2022)	Applications for Women's mHealth.	A scoping review and content analysis of privacy policies within the Apple operating system (iOS) and Google Play on the Android platform.	Based on European Union General Data Protection Regulation (GDPR): Children's age regulation or age restriction, personal data collection using consent, data sharing information i.e. behaviour tracking and location tracking, data accessibility i.e. deleting past data by request, data retention, 3rd party sharing, and data processing
11	(Mia et al., 2022)	Applications related to medicine, health, and fitness available on the Google Play Store.	An experimental design using android source code analysis framework to evaluate the HIPAA compliant	HIPAA security requirements are divided into three types: Administrative, Physical, and Technical with rule names: authorization, unique id, data encryption-decryption, audit control, data integrity, user authentication, and transmission security
12	(Ni et al., 2021)	Chronic disease Apps	A systematic search of mHealth to analyse the compliance to the Personal Information (PI) Security	The security requirements for personal information encompass various aspects, including: 1. General attributes, e.g., app coverage, policy revelation, and policy revisions. 2. Data collection and usage, encompassing rules for gathering and utilizing data for business functions and sensitive personal data. 3. Data storage and safeguarding, which involves ensuring secure storage, handling security incidents, and safeguarding against malware. 4. Data sharing and transmission, addressing entrusted handling, personal information sharing, its transfer

No	Source	Scope of App	The research aims and method	Security and Privacy Requirements
				and public disclosure, and cross-border transmission. 5. Data destruction, including storage duration, data deletion, and anonymization. 6. Entitlements of personal information subjects.
13	(Rosenfeld et al., 2017)	Availability of privacy policy in dementia Apps.	A systematic search related to dementia Apps and finding privacy concerns of the Apps.	The privacy concerns from dementia Apps: Recording Internet Protocol (IP) addresses; Storing cookies; Sharing data with business partners or third parties; Sharing data with marketers or advertisers; Selling data in cases of merger or acquisition; Disclosing data if legally obligated; Providing the option to delete or amend data upon request.
14	(Robillard et al., 2019)	Mental health Apps	A methodical exploration aimed at assessing the accessibility, comprehensibility, and privacy-oriented details of mental health Applications, achieved by analysing privacy policies and terms of agreement.	Content analysis of privacy policy stated: a statement for not selling data without user agreement, statement for not sharing user information with third parties, statement to guarantee of user's data information security, statement of data access that the user may be able to delete, and statement of specific laws that have been used for a privacy policy.
15	(Bining et al., 2022)	Apps for supporting cancer caregivers.	Examine the efficacy, worth, therapeutic capabilities, and security aspects of publicly available Applications designed to support unpaid cancer caregivers in fulfilling their responsibilities.	The mean quality score (MARS) was used to classify the level of quality and privacy. Privacy terms of use serve as reservoirs of information exposure, data confidentiality, data utilisation procedures, regulations concerning minors, and transparent data transmission, and notifications if data might be shared. While security terms of use are security to collect data, security of transmission, documentation of data exposure, and compliance.
16	(Flors-Sidro et al., 2021)	Mobile apps for diabetes	A partially automated application search module designed to retrieve privacy-related information from Android apps to analyse privacy aspects related to diabetes apps	Privacy-related feature: - access to private user data or control over the mobile device - sharing critical personal data (i.e precise location) - Third-party information - International data sharing
17	(Bachiri et al., 2016)	Applications for postnatal care.	Evaluation of the privacy policies within 30 postnatal care applications.	Policy Content Categories: 1. Data Collection and Disclosure: - Types of Collected Information - Reasons for Collection - Utilization and Sharing of Gathered Data - Engagement with Third-Party Services - Data Transmission 2. Security and Privacy: - Security Measures - Data Retention Practices - Privacy Concerns for Children - Usage of Cookies

No	Source	Scope of App	The research aims and method	Security and Privacy Requirements
				3. User Empowerment: - User Rights - Personal Data Control - Modifications to the Privacy Policy

Most of the research papers used observation of the privacy policy to assess mHealth security and privacy. Security and privacy features from observing policy are related to user access such as third-party transfer data permission, web-link for the privacy policy, advertising content, accessibility to location, storage, camera, contact, audio, etc., and policy text availability. Some articles assessed the policy content to measure the level of security and privacy. Amongst the articles, only 3 articles used the GDPR framework to evaluate the privacy and policy level, while 1 article reviewed the content using the HIPAA framework. Based on the current review, the assessment of the privacy policy which complies with the GDPR framework has 14 items of the privacy checklist such as identity of the data controller, identity of the representative, details of the Data Protection Officer (DPO), processing purposes, legal basis for processing, assessment of legitimate interests by the controller, recipients of personal data, international data transfers, data retention period, recognition of data subject rights, acknowledgment of the right to withdraw consent, right to lodge complaints, obligation to provide personal data, and presence of automated decision-making and profiling.

4.2. Security and Privacy Requirements for mHealth Privacy Policy

This subsection introduced a comprehensive set of requirements by categorising them into security and privacy domains. These domains were carefully structured to encompass various aspects and their critical requirements for the evaluation of mHealth app privacy policies.

The security aspect of data information is defined as the adequate controls to ensure the confidentiality, integrity, and availability of information (National Institute of Standards and Technology, 2020; Soenen & Academy, 2019). Based on the current review, the data transmission requirements are: providing secure transmissions such as using Hypertext Transfer Protocol Secure or HTTPS, password, user authentication and encryption, virus or malware protection, and handling security incidents (see Table 3).

Table 3. Security Aspect and Requirements of mHealth

Security Aspect	Requirements	Sources
Protection and transmission	Secure transmission	(Tangari et al., 2021), (Mia et al., 2022)
	Password, user authentication, and encryption	(Mia et al., 2022)
	Virus/malware protection and handling for security incidents	(Mia et al., 2022)

The privacy aspect of data information is described as the entitlement of a user to obtain information, manage their own data, and disconnect from individual data. Based on the current review, the privacy aspect is classified into three domains namely: consistency and transparency, data management and processing, and interconnected-data arrangement. The detailed requirements are explained in Table 4.

Table 4. Privacy Aspect and Requirements of mHealth

Privacy Aspect	Requirements	Sources
Consistency and Transparency	Data collection process: - Data processing is well-understood and informed either for primary uses or secondary uses - Request for data collection - Scope of data collection	(Hatamian et al., 2021), (Huckvale et al., 2019), (Tangari et al., 2021), (Parker et al., 2019), (Hendricks-Sturrup, 2022), (Alfawzan et al., 2022), (Bookert et al., 2022), (Flors-Sidro et al., 2021), (Levine et al., 2020)

Privacy Aspect	Requirements	Sources
Data management and processing	Type of information or data retrieved: - The type of information is well-understood - The rationale for collecting data	(Sunyaev et al., 2015), (Ni et al., 2021), (Bachiri et al., 2016)
	The legal action for protecting the data: - Specific laws or policies are informed (legal jurisdiction governing data processing) - Valid policy text (availability/readability) - Technical security measurement - Web link for a privacy policy	(Huckvale et al., 2019), (Parker et al., 2019), (Minen et al., 2018), (Ni et al., 2021), (Robillard et al., 2019),
	Data access: - Presence of Data Subject Rights - Availability of the Right to Revoke Consent - Permission to access location, contact, audio, media, etc. - A period that data will be stored or data retention - Ability to delete the data	(Hatamian et al., 2021), (Huckvale et al., 2019), (Tangari et al., 2021), (Bookert et al., 2022), (Benjumea et al., 2020), (Ni et al., 2021), (Rosenfeld et al., 2017), (Robillard et al., 2019), (Bachiri et al., 2016)
	Process consistency: - The process is maintained and consistent (privacy and security regulations are updated regularly) - Purposes for processing	(Huckvale et al., 2019), (Bachiri et al., 2016)
	Data transparency: - User control (notification) - Reason or rationale for data sharing - Recipients of personal data - Not sharing data without user agreement	(Hatamian et al., 2021), (Sunyaev et al., 2015), (Parker et al., 2019), (Benjumea et al., 2020), (Robillard et al., 2019), (Bachiri et al., 2016)
	Maintain data quality: - The availability of the user's right to file a complaint - Regular updates or maintenance or policy changes notification	(Hatamian et al., 2021), (Benjumea et al., 2020),
	Data authentication: - Data authentication such as identifiers i.e. email - Passwords - Obligation to provide personal data	(Hatamian et al., 2021), (Tangari et al., 2021), (Benjumea et al., 2020), (Rosenfeld et al., 2017), (Bachiri et al., 2016)
	Data disclosure: - Asserting non-identifiable data - The purpose of data storage - Data storage location	(Hatamian et al., 2021), (Huckvale et al., 2019), (Sunyaev et al., 2015), (Benjumea et al., 2020), (Ni et al., 2021), (Minen et al., 2018)
	Technical security procedure: - Anonymisation - secure servers and backup	(Huckvale et al., 2019), (Parker et al., 2019), (Benjumea et al., 2020)
	Procedures for vulnerable or at-risk users - Control by notification - Under age regulation	(Hatamian et al., 2021), (Huckvale et al., 2019), (Sunyaev et al., 2015), (Bookert et al., 2022), (Benjumea et al., 2020), (Alfawzan et al., 2022), (Bachiri et al., 2016)
Interconnected-data arrangement	Data arrangement identification - Identification of the Data Controller or Responsible Legal Entity - Identity Details of Data Controller, Representative, and Data Protection Officer (DPO)	(Hatamian et al., 2021), (Benjumea et al., 2020)
	Procedures (policy) for data sharing: - Permitted sharing - The App encouraged interaction between users and data sharing - App request for data sharing - Legal basis for the sharing process - Partners to share the data (advertiser, business partner, etc.)	(Hatamian et al., 2021), (Bookert et al., 2022), (Benjumea et al., 2020), (Minen et al., 2018), (Alfawzan et al., 2022), (Ni et al., 2021), (Rosenfeld et al., 2017), (Flors-Sidro et al., 2021)
	Procedures for data interconnection - Third-party information and approval - Information or detail of International transfer data - Guarantee for user data security	(Hatamian et al., 2021), (Sunyaev et al., 2015), (Bookert et al., 2022), (Benjumea et al., 2020), (Minen et al., 2018), (Alfawzan et al., 2022), (Ni et al., 2021), (Robillard et al., 2019), (Flors-Sidro et al., 2021)

5. Discussion

The review provides an overview of the literature concerning the evaluation of privacy and security in mHealth applications. These results suggest that the digitisation of information has a significant impact on the healthcare security and privacy requirements of providers. Our study showed most of the papers evaluate security and privacy with respect to mental health Apps such as depression, bipolar disorder, and dementia. Demand for privacy for mental health care has increased to improve access to care as well as the quality of enhanced recovery. Mental health services, which are limited in many countries, should be provided using effective interventions through healthcare facilities, community teams for mental health, family, and currently through computer applications. In a prior research investigation, it was discovered that mHealth technology utilised for mental health facilitates the gathering and storage of substantial quantities of sensitive data, which can be readily accessed over the network, both locally and remotely. This situation raises concerns about potential security breaches and infringements on privacy (Parker et al., 2019).

The privacy concern is increased not exclusively for mental health patients but also for different fields of healthcare such as chronic diseases such as diabetes and cancer Apps ((Bining et al., 2022; Flors-Sidro et al., 2021; Ni et al., 2021)). Although non-mental health Apps do not contain sensitive information, however, many mHealth Apps require personal information such as identity number, phone number, date of birth, health information, lab result, location, etc. Based on the current study, several Apps request access to a phone book, gallery, map, and data storage of the user's cellular phone (Bachiri et al., 2016; Russell et al., 2021). Based on the privacy act released by the Canadian Government, an institution must inform people about how their personal information will be used and who will receive it. Personal information may only be used for the purposes for which it was collected or for uses that are consistent with that purpose (Justice Law, 2007).

Numerous countries, particularly developed ones, have enacted privacy and data protection laws and regulations imposing stringent limitations concerning the gathering, handling, and revelation of personal data (Hughson et al., 2018). Consequently, organizations within these countries are obligated to implement security measures to safeguard personal data against accidental loss and unlawful misuse. In response to the demand for technical mechanisms to enforce legal mandates, several privacy policy languages have been developed to protect individuals' privacy. However, some developing countries still do not have security and privacy regulations today. This condition has brought impacted security protection where there is an increasing trend of cybercrime in the country (Aswandi et al., 2020).

Based on the current findings, App security requires protection of data transmissions such as secure transmission, password protection, and malware protection which can be prepared during the App development, while privacy requires consistency and transparency, data management and processing, and an interconnected-data arrangement. Based on current privacy assessment through policy text and App features, consistency and transparency could be provided through the availability of a data collection process, type of information or data retrieved, legal action for protecting data, providing data access, process consistency, data sharing transparency, and data quality maintenance (Huckvale et al., 2019; Minen et al., 2018; Robillard et al., 2019). Transparency and consistency of the data collection and process is important to the communication systems that transmit data which provide detailed process explanations and legal aspects to increase trustworthiness. According to (Lamonica et al., 2021; Paul et al., 2018) the lack of transparency in terms of data privacy within applications has resulted in low rates of adoption of such contact tracing applications in developed countries.

The other requirement for the privacy policy of the mHealth Apps is data management and processing which consist of the availability of data disclosure, technical security procedure, and procedures for vulnerable or at-risk users (Benjumea et al., 2020; Huckvale et al., 2019; Minen et al., 2018; Sunyaev et al., 2015). The data processes are made up of a personal data collection, storage, processing, transfer, and deletion. Data management is an important aspect of personal data processing because it allows for the identification of authorised access, the authentication of involved parties, links to the data sets, the expression of data ownership, and the delegation of rights to third parties. This aspect pertains to Article 13 of GDPR which stipulates that when personal data concerning a data subject is collected directly from the data subject, the data controller is obligated to furnish the data subject with all necessary information at the moment of data collection (Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016).

The principles of data privacy in the interconnected digital landscape of the Internet pose challenges, given that information can be extracted from diverse digital origins including social media, email servers, websites, blogs, online transactions, and virtual inquiries. Based on this research, the last requirement for privacy is an interconnected-data arrangement which is connected to the availability of data arrangement identification, procedures (policy) for data sharing, and procedures for data interconnection (Benjumea et al., 2020; Minen et al., 2018; Robillard et al., 2019; Sunyaev et al., 2015). This aspect is related to article 14 in GDPR when personal data has not been acquired directly from the data subject or related to data sharing (Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016).

Our identified privacy requirements exhibit notable similarities with established principles in prior privacy assessment frameworks, such as those outlined by (Mnjama et al., 2017; Yaqoob et al., 2020). These commonalities underscore the enduring importance of transparency, data disclosure, and user rights across diverse domains. However, our study revealed specific nuances intrinsic to mHealth app privacy, emphasizing the need for more detailed guidelines on data retention periods and international data transfers, areas that may require further attention in evolving privacy assessment frameworks.

While policy analysis provides valuable insights into regulatory compliance and data handling guidelines, it does present limitations in evaluating the practical implementation of these policies. A study by (Bally & Cesuroglu, 2020) integrate technical implementation with stakeholder perspectives. Neglecting the examination of technical safeguards and user perceptions may overlook critical aspects of mHealth app privacy. A comprehensive assessment that combines policy analysis with technical evaluations and user perspectives would offer a more holistic understanding of privacy in this context.

To enhance mHealth privacy, there are specific guidelines for regulators and developers. These include the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the NIST Privacy Framework, ISO 27701, the HITRUST Common Security Framework (CSF), the US Food and Drug Administration (FDA) Guidelines, the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines, and various National and Regional Laws. Many countries and regions have their own healthcare and data protection laws that may apply to mHealth apps. For instance, Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA), California has the California Consumer Privacy Act (CCPA), and Indonesia has Undang-undang Pelindungan Data Pribadi (Personal Data Protection Law).

6. Research Implications

The review results have implications for regulators as well as developers who are involved in security and privacy assessment to build a strategic plan for an organisation. Regulatory authorities could also utilise the outcomes for assessment tools to measure the security and privacy policy of the applications and provide a standard tool as the self-assessment tool for the App provider.

7. Conclusions

Security and privacy policy are important to enhance safeguarding the personal data of the user as well as increase trustworthiness amongst App users. The results of the current study show that a privacy policy for mHealth requires: (1) Consistency and transparency, (2) data management and processing (3) interconnected data arrangement. Consistency and transparency could be provided through the availability of a data collection process, type of information or data retrieved, legal action for protecting data, providing data access, process consistency, data sharing transparency, and data quality maintenance, while the data management and processing consists through the availability of data disclosure, technical security procedures, and procedures for vulnerable or at-risk users. The other requirement is an interconnected-data arrangement through the availability of data arrangement identification, procedures (policy) for data sharing, and procedures for data interconnection.

To further enhance the trustworthiness of mHealth apps and privacy policies, we recommend considering regulations to ensure the completeness and standardisation of privacy policy. Additionally, evaluating and promoting privacy awareness among mHealth users can play a pivotal role in enhancing trust. Looking ahead, future research directions should focus on exploring novel and critical privacy policy requirements emerging in the evolving landscape of mHealth apps. These efforts will contribute to the ongoing development of robust privacy policies and the cultivation of user trust in this rapidly advancing field.

Acknowledgement

This research was supported by the Research Management Centre of Universitas Islam Negeri Syarif Hidayatullah Jakarta in the Inter-University Collaboration Research Cluster [SK KPA No: UN.01/KPA/223/2022].

References

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis. *JMIR MHealth and UHealth*, *10*(5), e33735. https://doi.org/10.2196/33735

American Psychiatric Association. (2022). *The App Evaluation Model.*

Aswandi, R., Muchsin, P. R., & Sultan, M. (2020). *Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)*. *3*(2), 167–190.

Bachiri, M., Idri, A., Fernández-Alemán, J. L., & Toval, A. (2016). Mobile personal health records for pregnancy monitoring functionalities: Analysis and potential. *Computer Methods and Programs in Biomedicine*, *134*, 121–135. https://doi.org/10.1016/j.cmpb.2016.06.008

Bally, E. L. S., & Cesuroglu, T. (2020). Toward Integration of mHealth in Primary Care in the Netherlands: A Qualitative Analysis of Stakeholder Perspectives. *Frontiers in Public Health*, *7*. https://doi.org/10.3389/fpubh.2019.00407

Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., & Carrasco, A. (2020). Assessment of the fairness of privacy policies of mobile health apps: Scale development and evaluation in cancer apps. *JMIR MHealth and UHealth*, *8*(7), 1–20. https://doi.org/10.2196/17134

Bining, M., Wasserman, S., Brahim, L. O., Belzile, E., Magalhaes, M., & Lambert, S. D. (2022). An Evaluation of Publicly Available Smartphone Apps to Support Unpaid Cancer Caregivers. *Journal of Pain and Symptom Management*, *63*(3), 430–439. https://doi.org/10.1016/j.jpainsymman.2021.09.017

Bookert, N., Bondurant, W., & Anwar, M. (2022). Data practices of internet of medical things: A look from privacy policy perspectives. *Smart Health*, *26*(September), 100342. https://doi.org/10.1016/j.smhl.2022.100342

Centers for Medicare and Medicaid Services. (2021). *HIPAA Basics for Providers : Privacy , Security , & Breach Notification Rules* (Issue May, pp. 1–11). Medicare Learning Network.

Cornet, V. P., & Holden, R. J. (2018). Systematic review of smartphone-based passive sensing for health and wellbeing. *Journal of Biomedical Informatics*, *77*, 120–132. https://doi.org/10.1016/j.jbi.2017.12.008.Systematic

Proposed Rule Standards for Privacy of Individually Identifiable Health Information, 64 Federal Register (1999).

Dinh-Le, C., Chuang, R., Chokshi, S., & Mann, D. (2019). Wearable health technology and electronic health record integration: Scoping review and future directions. *JMIR MHealth and UHealth*, *7*(9). https://doi.org/10.2196/12861

Elliot Mbunge, John Batani, Goabaone Gaobotse, & Benhildah Muchemwa. (2022). Virtual healthcare services and digital health technologies deployed during coronavirus disease 2019 (COVID-19) pandemic in South Africa: a systematic review. *Global Health Journal*.

Flors-Sidro, J. J., Househ, M., Abd-Alrazaq, A., Vidal-Alaball, J., Fernandez-Luque, L., & Luis Sanchez-Bocanegra, C. (2021). Analysis of diabetes apps to assess privacy-related permissions: systematic search of apps. *JMIR Diabetes*, *6*(1), 1–14. https://doi.org/10.2196/16146

Hatamian, M., Wairimu, S., Momen, N., & Fritsch, L. (2021). A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. In *Empirical Software Engineering* (Vol. 26, Issue 3). Empirical Software Engineering. https://doi.org/10.1007/s10664-020-09934-4

Hendricks-Sturrup, R. (2022). Pulse Oximeter App Privacy Policies during COVID-19: Scoping Assessment. *JMIR MHealth and UHealth*, *10*(1), 1–10. https://doi.org/10.2196/30361

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Network Open*, *2*(4), 1–10. https://doi.org/10.1001/jamanetworkopen.2019.2542

Hughson, J. A. P., Oliver Daly, J., Woodward-Kron, R., Hajek, J., & Story, D. (2018). The rise of pregnancy apps and the implications for culturally and linguistically diverse women: Narrative review. In *JMIR mHealth and uHealth* (Vol. 6, Issue 11). https://doi.org/10.2196/mhealth.9119

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on Android platform. *Telematics and Informatics*, *35*(5), 1335–1354. https://doi.org/10.1016/j.tele.2018.03.005

Justice Law. (2007). Access to Information Act and Privacy Act: Annual Report 2006-2007. In *Government of Canada*.

Lagan, S., Sandler, L., & Torous, J. (2021). Evaluating evaluation frameworks: A scoping review of frameworks for assessing health apps. *BMJ Open*, *11*(3). https://doi.org/10.1136/bmjopen-2020-047001

Lamonica, H. M., Roberts, A. E., Lee, G. Y., Davenport, T. A., & Hickie, I. B. (2021). Privacy practices of health information technologies: Privacy policy risk assessment study and proposed guidelines. *Journal of Medical Internet Research*, *23*(9). https://doi.org/10.2196/26317

Levine, D. M., Co, Z., Newmark, L. P., Groisser, A. R., Holmgren, A. J., Haas, J. S., & Bates, D. W. (2020). Design and testing of a mobile health application rating tool. *Npj Digital Medicine*, *3*(1), 1–8. https://doi.org/10.1038/s41746-020-0268-9

Liu, Q., & Zhang, T. (2023). Deep learning technology of computer network security detection based on artificial intelligence. *Computers and Electrical Engineering*, *110*. https://doi.org/10.1016/j.compeleceng.2023.108813

Mia, M. R., Shahriar, H., Valero, M., Sakib, N., Saha, B., Barek, M. A., Faruk, M. J. H., Goodman, B., Khan, R. A., & Ahamed, S. I. (2022). A comparative study on HIPAA technical safeguards assessment of android mHealth applications. *Smart Health*, *26*(September), 100349. https://doi.org/10.1016/j.smhl.2022.100349

Minen, M. T., Stieglitz, E. J., Sciortino, R., & Torous, J. (2018). Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. *Headache*, *58*(7), 1014–1027. https://doi.org/10.1111/head.13341

Mnjama, J., Foster, G., & Irwin, B. (2017). A privacy and security threat assessment framework for consumer health wearables. *2017 Information Security for South Africa - Proceedings of the 2017 ISSA Conference*, *2018-January*, 66–73. https://doi.org/10.1109/ISSA.2017.8251776

Morera, E. P., de la Torre Díez, I., Garcia-Zapirain, B., López-Coronado, M., & Arambarri, J. (2016). Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide. *Journal of Medical Systems*, *40*(6). https://doi.org/10.1007/s10916-016-0513-6

Nass, S. J., Levit, L. A., & Gostin, L. O. (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. In *National Academies*. National Academies Press (US). https://doi.org/10.17226/12458

National Institute of Standards and Technology. (2017). NISTIR 8062: An introduction to privacy engineering and risk management in federal systems. *NIST Interagency Report*, 49.

National Institute of Standards and Technology. (2020). NIST Privacy Framework. In *January 16, 2020*.

Ni, Z., Wang, Y., & Qian, Y. (2021). Privacy Policy Compliance of Chronic Disease Management Apps in China: Scale Development and Content Evaluation. *JMIR MHealth and UHealth*, *9*(1), e23409. https://doi.org/10.2196/23409

Nurgalieva, L., O'Callaghan, D., & 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

Pang, P. C. I., McKay, D., Chang, S., Chen, Q., Zhang, X., & Cui, L. (2020). Privacy concerns of the Australian My Health Record: Implications for other large-scale opt-out personal health records. *Information Processing & Management*, *57*(6), 102364. https://doi.org/10.1016/J.IPM.2020.102364

Parker, L., Halter, V., Karliychuk, T., & 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*(November 2018), 198–204. https://doi.org/10.1016/j.ijlp.2019.04.002

Paul, N., Tesfay, W. B., Kipker, D. K., Stelter, M., & Pape, S. (2018). Assessing privacy policies of internet of things services. *IFIP Advances in Information and Communication Technology*, *529*, 156–169. https://doi.org/10.1007/978-3-319-99828-2_12

Robillard, J. M., Feng, T. L., Sporn, A. B., Lai, J. A., Lo, C., Ta, M., & Nadler, R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*, *17*(March), 100243. https://doi.org/10.1016/j.invent.2019.100243

Rosenfeld, L., Torous, J., & Vahia, I. V. (2017). Data Security and Privacy in Apps for Dementia: An Analysis of Existing Privacy Policies. *American Journal of Geriatric Psychiatry*, *25*(8), 873–877. https://doi.org/10.1016/j.jagp.2017.04.009

Rudnytskyi, V., Korchenko, O., Lada, N., Ziubina, R., Wieclaw, L., & Hamera, L. (2022). Cryptographic encoding in modern symmetric and asymmetric encryption. *Procedia Computer Science*, *207*, 54–63. https://doi.org/10.1016/J.PROCS.2022.09.037

Ruotsalainen, P., & Blobel, B. (2020). Health information systems in the digital health ecosystem—problems and solutions for ethics, trust and privacy. *International Journal of Environmental Research and Public Health*, *17*(9), 1–16. https://doi.org/10.3390/ijerph17093006

Russell, C. R., Zigan, C., Wozniak, K., Soni, K., Hill Gallant, K. M., & Friedman, A. N. (2021). A Systematic Review and Qualitative Analysis of Existing Dietary Mobile Applications for People With Chronic Kidney Disease. *Journal of Renal Nutrition*, *32*(4), 382–388. https://doi.org/10.1053/j.jrn.2021.06.006

Shore, J. H., Yellowlees, P., Caudill, R., Johnston, B., Turvey, C., Mishkind, M., Krupinski, E., Myers, K., Shore, P., Kaftarian, E., & Hilty, D. (2018). Best Practices in Videoconferencing-Based Telemental Health April 2018. *Telemedicine and E-Health*, *24*(11), 827–832. https://doi.org/10.1089/tmj.2018.0237

Soenen, P., & Academy, Q. A. (2019). *Privacy Information Management with ISO 27701 Overview of the ISO 27701 Who should implement ISO 27701 ? GDPR certification ISO 27701 - an extension to ISO 27001. May 2018*, 1–17.

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, *22*(e1), e28–e33. https://doi.org/10.1136/amiajnl-2013-002605

Tangari, G., Ikram, M., Ijaz, K., Kaafar, M. A., & Berkovsky, S. (2021). Mobile health and privacy: Cross sectional study. *The BMJ*, *373*. https://doi.org/10.1136/bmj.n1248

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union (2016).

Xu, K., Zhang, W., & Yan, Z. (2018). A privacy-preserving mobile application recommender system based on trust evaluation. *Journal of Computational Science*, *26*, 87–107. https://doi.org/10.1016/j.jocs.2018.04.001

Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P., & Wang, X. S. (2013). AppIntent: Analyzing sensitive data transmission in Android for privacy leakage detection. *Proceedings of the ACM Conference on Computer and Communications Security*, 1043–1054. https://doi.org/10.1145/2508859.2516676

Yaqoob, T., Abbas, H., & Shafqat, N. (2020). Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices. *IEEE Journal of Biomedical and Health Informatics*, *24*(6), 1752–1761. https://doi.org/10.1109/JBHI.2019.2952906