IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 11, 2020, accepted May 25, 2020, date of publication June 4, 2020, date of current version June 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2999934

Security and Privacy of mHealth Applications: A Scoping Review

LEYSAN NURGALIEVA[1], DAVID O'CALLAGHAN[2], AND GAVIN DOHERTY[1]
[1]Trinity College Dublin, Ireland
[2]SilverCloud Health, Dublin 8, D08 DR9P Ireland

Corresponding author: Leysan Nurgalieva (leysan.nurgalieva@tcd.ie)

This work was supported in part by the EU Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie under Grant 754489, in part by the Science Foundation Ireland under Grant 13/RC/2094, and in part by the European Regional Development Fund through the Southern and Eastern Regional Operational Programme to Lero—the Irish Software Research Centre.

ABSTRACT While digital health or mHealth applications (apps) have become accessible resources for the support of personal health, the privacy and security of users' data have been the subject of concern and controversy. As large numbers of mHealth apps are created and are increasingly widely used by people with various health conditions, it is crucial to have clear and valid methods for evaluating the data practices within them. Recent regulatory initiatives such as the European Union's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) have had the effect of raising awareness and establishing a minimal set of expectations. However, they do not in themselves address the issue of the development of systems which meet privacy and security requirements. There is a growing body of research on evaluation techniques and frameworks to support the assessment of the privacy and security of health apps, and guidelines to support their design. However, it can be challenging to navigate this space and choose appropriate techniques for a given context. Addressing this issue, this paper examines the recent literature on security and privacy of m-Health applications, using a scoping review methodology. It analyses data security and privacy evaluation techniques and frameworks that have been proposed for mHealth applications, as well as relevant research-based design recommendations. This work consolidates recent research on the topic to support researchers, app designers, end users, and healthcare professionals in designing, evaluating, recommending and adopting mHealth applications.

INDEX TERMS Digital health, human computer interaction, data privacy, data protection, data security, mHealth.

I. INTRODUCTION

There is a growing body of literature that recognises the potential of mobile applications (apps) to improve access to healthcare and provide real-time monitoring and self-management of various health conditions [1]–[3]. For instance, mHealth apps have become popular resources for mental health support as an accessible alternative or adjunct to face-to-face therapy [4]. They are increasingly widely used, both independently and following the recommendation of health professionals [5].

However, there is also growing awareness and concern about the privacy of information within mHealth apps, which may be compromised by malicious hacking, through commercial data-sharing practices [6]–[9], or devices being stolen [10]. Privacy implies the individual's right to maintain control over and be free from intrusion into their private life, as defined by the European Convention on Human Rights and other national laws [11]. It should be ensured in digital health services. Personal data protection is a distinct right under the European Union (EU) Charter of Fundamental Rights.

While mHealth apps necessarily involve the processing of sensitive information, potentially by several entities, safeguards may be used. However, safeguarding measures such as de-identification of user data provided to third parties can potentially be circumvented. For example, de-identified information can be combined with data from other sources (e.g. social media, public records) [8] and poses various risks that are particularly important for users with health difficulties. These range from unvetted or intrusive targeted advertising to inferences about an individual's behaviour and health condition, which might affect employment or promotion prospects [12].

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

Existing US regulations in the space of digital health include those of the Food and Drug Administration (FDA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides a Privacy Rule for safeguarding medical information [13]. However, HIPAA has been recently criticised for allowing too much access to data and not protecting patients from new threats to their data [14], [15].

The European Union's General Data Protection Regulation (GDPR) [16] – which was approved by the European Parliament in April 2016 and came into force in May 2018 – and the California Consumer Privacy Act (CCPA) that came into force from 2020 have triggered further interest in privacy and data protection, both for online services and health care organisations. While many mHealth app developers updated their privacy practices to comply with the GDPR, others stated that "their practices would not provide GDPR-level protection to its users but would adhere to local privacy regulations even if app users were 'visiting' the app from other jurisdictions" [17, p.202]. Furthermore, the "privacy as compliance" reaction of many organizations does not align with the "data protection by design and by default" requirement of GDPR and related "Privacy by Design" (PbD) principles, which advocate that privacy requirements be taken into consideration from the very beginning of product design and development [18]. The dominant privacy model today is still based on privacy notices, followed by an agreement to such terms. This frames consent *as choice*, but this approach "no longer safeguards consumer privacy interests with modern health technologies" [19, p.1507].

Thus, while regulations have had an impact on the field, the degree of compliance is uneven, and the directives only partially cover the security and privacy issues facing users and developers of digital health apps.

Hence, it is crucial to have clear procedures for evaluating the data practices of mHealth applications. Existing techniques and frameworks can guide professionals and patients through the process of assessing mHealth apps and identifying the privacy and security risks associated with them. However, in this rapidly expanding field, it can be challenging to choose which of the many available techniques to employ, given the evaluation objectives, mHealth app lifecycle stage, and available expertise.

This scoping review focuses on the following research questions (RQs):

RQ1. What research-based evaluation frameworks and evaluation techniques are available to assess the security and privacy of mHealth applications? This work aims to characterise frameworks and evaluation techniques, the strategies used to generate and validate them and identify the target stakeholders and development context. By providing an overview of the current landscape of evaluation methods, the results of this review can provide support for choosing appropriate methods at each stage of the mHealth development process and highlight areas where further research is needed.

RQ2. What research-based guidelines, recommendations, and practices are available to support security and/or privacy (S/P) in the development of mHealth applications? This review examines research-derived design recommendations, analysing their scope and form, to provide a classification and consolidation of research-based security and privacy design guidelines for mHealth applications.

This study reviews and analyses data security and privacy evaluation guidelines and frameworks for mHealth apps published in the recent literature, covering the period from April 2016 – when the GDPR was introduced – to August 2019. The findings are intended for app designers, clinicians, and patient groups to consult when designing and assessing health applications. The focus of this work is on security and privacy, addressing data protection as well, as it relevant to both in the context of mHealth apps.

The paper is organised as follows: Section II includes an overview of the background literature on security and privacy of mHealth interventions; Section III describes the methodology of the literature review; Section IV presents the results of the analysis of the 83 included studies; Section V presents discussion of the review findings; and Section VI outlines some final considerations, limitations, and pointers for the future research.

II. BACKGROUND

There has been much recent research on mobile health (mHealth) apps, as large numbers of them are being developed to address a wide range of health-related conditions and goals, such as monitoring symptoms and obtaining professional health support remotely. There is a massive amount of "apptimism", a term coined by Wyatt [20]; health apps are endorsed by healthcare organisations, governments, and recommended by clinicians as an inexpensive and accessible adjunct to therapy, or to support patients with particular health conditions. Health apps play an increasing role in patients' lives, and the growing technological sophistication of smartphones has enabled the delivery of new functionalities and interventions.

However, the defining feature of digital health concerns data rather than technology. From a wide range of sources, such as wearable, portable or even implantable devices, digital health products generate large sets of patient data. They circulate it to devices and/or health professionals (who analyse and make sense of the data), creating opportunities for more precise diagnostics and more personalised healthcare delivery.

These advances have also raised concerns regarding the quality of novel digital health interventions, their efficacy, general safety, and the accuracy of marketing claims made about them [21], [22]. Furthermore, the generation of large amounts of new personal patient data increases the significance and severity of security and privacy risks. Vulnerabilities regarding privacy and security may result in breaching the confidentiality of consumers' data [6], which can lead to financial losses, discrimination, stress, dissatisfaction [23],

or even delays in seeking effective treatment due to perceived privacy risks [24], [25]. The current situation is alarming, as recent studies report on privacy violations being a common occurrence with health and wellbeing (HWB) applications [26], [27]. These risks could be harmful not only to the patients whose privacy is threatened, but also to the long term development of applications, which can provide patient benefit, and for providers and healthcare professionals, through reputation damage or compromised credibility [28]. One of the reasons for the prevalence of health apps that put privacy of consumers at risk is the lack of compliance with existing regulations.

There are many regulations – regional and global – that are relevant to digital health. By setting out the obligations for parties processing personal data, including the legal bases for processing, data protection principles, and accountability measures, they establish a legislative basis for protecting fundamental rights of mHealth consumers. However, it is not always easy to recognise which of them apply to a particular health application.

Currently, several key regulations play an important role when it comes to mHealth apps. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is US legislation that provides data privacy and security provisions for safeguarding medical information. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and it sets limits and conditions on the use and disclosure of patient information [13]. Another relevant US regulation is the US Children's Online Privacy Protection Act (COPPA), which provides a federal legal framework to protect the online privacy of children under the age of 13 and forbids the gathering of personal information from them without express consent from a parent or legal guardian [29]. The most recent US regulation is the California Consumer Privacy Act (CCPA) which went into effect on January 2020, and provides California residents with greater transparency and protection of personal data, for instance, ensuring ''the right to know where data is collected and to whom it is sold, as well as the right to disclosure'' [30, p.94].

The regulatory framework of the US Food and Drug Administration (FDA) has been traditionally concerned with computerised devices intended for medical use. The ''medical device'' label (as assigned by the manufacturer) means that the product – hardware or a software application – is recognised by official bodies and intended for use in ''the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease'', and conformity to regulation must be shown [31].

In comparison, the European regulatory framework for medical devices operates through Conformité Européenne (CE) certification and is recognised as a more flexible approach that allows faster market access for certain medical devices. However, its decentralised approach is criticised for hindering ''the collection and analysis of safety data'' and exposing patients to risks [32, pp.124-125].

MHealth applications might fall into either ''medical'' or ''health'' app categories, as there is often no clear dividing line between them. The differentiation here is critical since both classes have different kinds of inherent risks and limitations [33], which indicates the need for a set of clear and applicable privacy and security evaluation criteria that go beyond categorisation but rather deal with the data practices within individual mHealth apps. Apps not intended for medical use are not currently regulated by the FDA in the US, for example, and are subject to very little oversight. To address this issue, in January 2019, the FDA launched a precertification program to help address the regulatory challenges posed by novel medical software [34]. This attempts to address developments in the digital health landscape by allowing some level of oversight to be provided, but without regulatory review of individual apps.

Another recent regulation within the European Union is the General Data Protection Regulation 2016/679 (GDPR) which came into force in May 2018, replacing its predecessor, the Data Protection Directive 95/46/EC. Unlike 95/46/EC, which was implemented through national data protection laws, GDPR is directly applicable in each EU member state. Under GDPR, data subjects must receive notice about collection and use of their data, and all processing of their data requires a legal basis. The regulation also places stricter requirements on the handling of sensitive data such as health records.

However, there are recognized problems with clarity, comprehension, and implementation of standards and regulations. Legal texts for software requirements may have issues with vagueness and incompleteness, together with ambiguities at lexical, syntactic, semantic, and referential levels; this makes it difficult for software engineers to implement compliant software [35].

Despite the increased prominence of privacy concerns and regulations, relevant laws are continually violated because consumers and regulators lack the tools to know when this is happening.

While spatial aspects of privacy such as visibility or location are often prioritised, temporal aspects are also important to consider, as every spatial description has a temporal aspect: ''when we discuss being in public or private space, time is always implied'' [36, p.17]. The costs of a data breach (time, effort, and other organisational resources) can also vary according to the time of the offence. Violations might require different protection mechanisms at the moment of data handling, compared to data breach resolution [37]. Even after patient data leaves the system, there might also be more indirect ways for privacy to be violated. For instance, sensitive personal information can be derived from analysing social media data [38] or by cross-referencing sets of ''de-identified'' data [39].

Addressing these challenges in the digital health field, several authors have proposed evaluation methods and tools (e.g. Mobile App Rating Scale (MARS) [40], Enlight assessment tools [41]) that assess various dimensions and

characteristics of mHealth interventions, such as usability, content, user engagement, and available research evidence. One of them is a privacy impact assessment (PIA), which can be defined as ''a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme'' [42]. However, a PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project, and should continue until and even after the project has been deployed [43]. A Data Protection Impact Assessment (DPIA) is also a requirement under GDPR for ''high risk'' activities involving personal data. These techniques are useful, as they facilitate multi-dimensional and thorough evaluations of health apps. However, it is not always easy to find and choose specific evaluation techniques that address the security and privacy of mHealth apps. Research-based evaluation and design recommendations often fall short of providing clear guidance for digital health stakeholders, including app developers and consumers.

The objective of this review is to provide an overview of current research-based security and privacy standards, guidelines, and evaluation frameworks relevant to the development of health apps. It aims to provide support for choosing security and privacy evaluation frameworks and guidelines for mHealth apps, addressing risks posed to developers, providers, patients and the public. The study will inform efforts that aim to improve the quality of mHealth apps and will provide a foundation for further research on producing actionable guidelines for developers and adopters.

III. METHODS

This study has been undertaken as a scoping review, which involves the synthesis and analysis of the existing research literature with the aim of providing greater conceptual clarity about a specific phenomenon [44]. The first phase consisted of identifying the articles to be reviewed. A systematic search was conducted with the Scopus,[1] PubMed, and ProQuest databases on the 6th of August 2019, as these contained papers from conference proceedings and journals most relevant to the areas of mHealth and human computer interaction (HCI), including the main titles of publishers such as ACM,[2] IEEE,[3] and Journal of Medical Internet Research (JMIR).

A. IDENTIFICATION PHASE

For each database, the titles and abstracts of every article were searched for following keywords: ''health'', ''app'' OR ''application'', ''security'' OR ''privacy''.[4] The search was performed on the 6th of August, 2019 and covered research articles written in English and published between April 2016[5] and August 2019. Given the rapid growth and development of the mHealth application space in recent years, we wished to focus on recent literature and the current regulatory landscape.

B. SCREENING PHASE

In the screening phase, we evaluated which of the identified articles contained relevant content for the review based on the following three inclusion criteria, considered independently:

- Security and/or privacy of smartphone health apps, where security and privacy is a substantive focus, not just mentioned in passing.
- Papers that present a contribution in the form of frameworks, evaluation techniques or practices[6] to identify risks and/or ensure security and/or privacy in health smartphone apps AND papers that present a contribution in a form of guidance, best practices, frameworks, or examples of ensuring security and privacy in health smartphone apps.
- Papers focused on end-user centric mHealth interventions.

Papers were excluded if they met any of the following criteria:

- Wearable device-oriented papers where the focus is on data transmission from the device rather than data usage within an app.
- Papers focused on specific security mechanisms such as face recognition.
- Papers focused on the aggregation of large sets of health data at a population level.
- Papers on apps to be used by medical staff rather than end-users/patients.

During this phase, the first author screened the content of each article's abstract and tagged it with either *Yes*, *No*, or *Maybe*. While *No* and *Yes* indicated exclusion or inclusion based on the defined criteria accordingly, *Maybe* suggested that the article could contain privacy and/or security evaluation techniques or the techniques to ensure privacy and/or security of mHealth applications. The inclusion of this category of papers was resolved during weekly meetings of the first and the third authors.

C. EXTRACTION PHASE

At the extraction phase, each article was evaluated in detail. For each article, we extracted the proposed privacy and/or security evaluation frameworks and methods and design guidelines (if available).

To keep records organised during the classification and filtering process, we applied several data management tools. As a tool for easier collaboration and collective work, shared spreadsheets were used to store the records obtained from

[1] Full Scopus database, not restricted to the medical category
[2] 65 ACM sources in Scopus
[3] 329 IEEE sources in Scopus
[4] Full search queries used in this scoping review are presented in the Appendix VI
[5] GDPR was approved by both the European Parliament and the European Council in April 2016 [45]
[6] The definition of evaluation techniques applied is explained in Section II

reviewed articles as well as to discuss the data and make annotations. A structured coding sheet was used to store information for each selected article. Coding parameters were the following: date and venue of publication, short summary of the contributions, target health conditions if any, pre-studies (that guided the creation/definition of the proposed evaluation frameworks and techniques, and design guidelines) and post-studies (that applied or validated the contributions) including data about subjects (size, age, stakeholder group), if available.

D. ANALYSIS PHASE

In this phase, we performed a qualitative analysis, i.e. thematic analysis of the extracted information, to categorise the evaluation techniques and practices to ensure security and/or privacy of mHealth application. The coded data were then used to address the research questions that guided the literature review.

To perform the thematic analysis, based on their primary contribution, we categorised papers in three groups and analysed the findings accordingly: articles that provide security and/or privacy evaluation techniques, evaluation frameworks, and articles that propose design guidelines and recommendations.

Next, we discuss the methods used to evaluate each of the groups.

1) ANALYSIS OF EVALUATION FRAMEWORKS

Privacy evaluation frameworks can be defined as comparing the system to a ''coherent set of actionable principles to protect patients' health information privacy'' [46, p.3]. Similarly, the objectives of a security evaluation framework can be described as to evaluate a system's ability to fulfil the stakeholders' security requirements and to identify potential risks [47].

Analysis of evaluation frameworks for health information systems followed the methodology proposed by [48]. It was based on the following questions: objective of the evaluation (why?), which stakeholders' perspective is to be evaluated (who?), which phase in the system development lifecycle is addressed (when?), focus of evaluation and specific artefacts related to mHealth apps (what?), and assessment methods (how?).

2) ANALYSIS OF SECURITY AND/OR PRIVACY EVALUATION TECHNIQUES

Following the work of Prat *et al.* [49] and their taxonomy of evaluation methods of information systems, we adopted and adjusted the following characteristics:

- The ''How'' of evaluation: the methods that lead to the suggested evaluation, evaluation techniques and tools used to conduct a study, level of evaluation (*ex-ante* evaluation or *ex-post* evaluation).
- The ''What'' of evaluation: the objectives or artefacts of evaluation, the hierarchy of evaluation criteria if specified by the authors.

In addition to these two dimensions, we also coded the stakeholders who would benefit from the suggested evaluation techniques, and the moment in the app lifecycle at which the evaluation should be applied.

3) ANALYSIS OF DESIGN GUIDELINES

In this literature review, we follow the definition of ''design guidelines'' of Dix and colleagues [50]. They broadly define them as the ''direction for design, in both general and more concrete terms, in order to enhance the interactive properties of the system''. Informed by this definition, we consider design guidelines as: guidance, practices or recommendations that can inform stakeholders in the development of secure and private mHealth applications.

Design recommendations extracted from the review corpus were evaluated based on their origin (including study methods used to generate them), their security and/or privacy focus, target stakeholders, and the form of design guidance provided. We also coded whether the recommendations were validated, e.g. if the paper included procedures or experiments applying the proposed design guidelines.

Initially, the guideline categories were extracted as indicated in the original papers. As the next step, all three authors revised the list of extracted categories and jointly aggregated them in the final taxonomy depicted in Figure 1.

IV. RESULTS

This section presents the results of the scoping review following the initial research questions.

A. STUDY SELECTION AND DATA EXTRACTION

The initial search in the *Identification phase* generated 628 papers across the three databases. After removing duplicates, the search yielded a set of 424 unique articles. As this scoping review was restricted to peer reviewed articles, the next stage included removing proceedings, editorial and opinion papers, news articles, books and book chapters, theses, clinical case paper, and papers from questionable venues (6 documents), which resulted in a set of 360 peer reviewed research papers. Reviews were not excluded but none were found in the search results.

During the *Screening phase*, the title and abstract of these 360 articles were evaluated and resulted in 176 articles that were considered as potentially eligible. The evaluation included checking towards the exclusion and inclusion criteria and the definition of guidelines presented in Section III.

In the *Eligibility phase*, a full-text analysis of these articles was performed to assess whether they met the inclusion criteria. This analysis excluded four more articles due to unavailability of the full text (3 papers) or supplementary data (1 paper), even after contacting the authors. The process followed for filtering relevant papers can be seen in the flow diagram in Figure 2.

Finally, during *Data extraction* phase (''Included'' in Figure 2), the corpus of 83 included articles was further reviewed to extract and code relevant information and

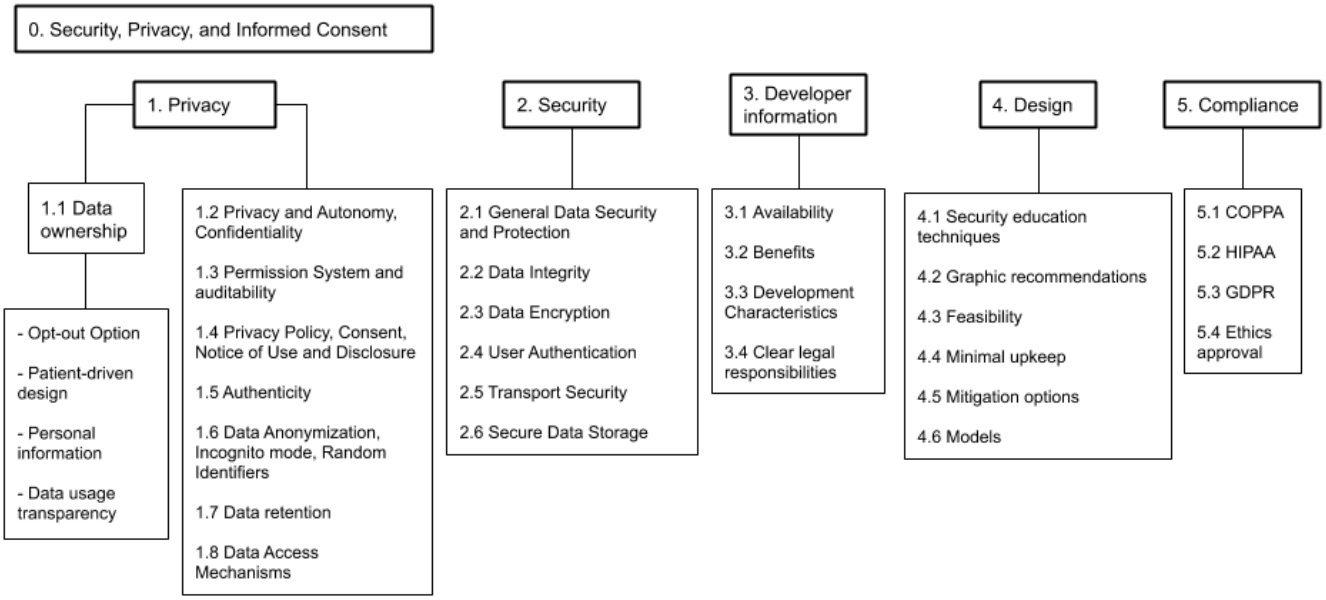

FIGURE 1. Design guideline taxonomy.

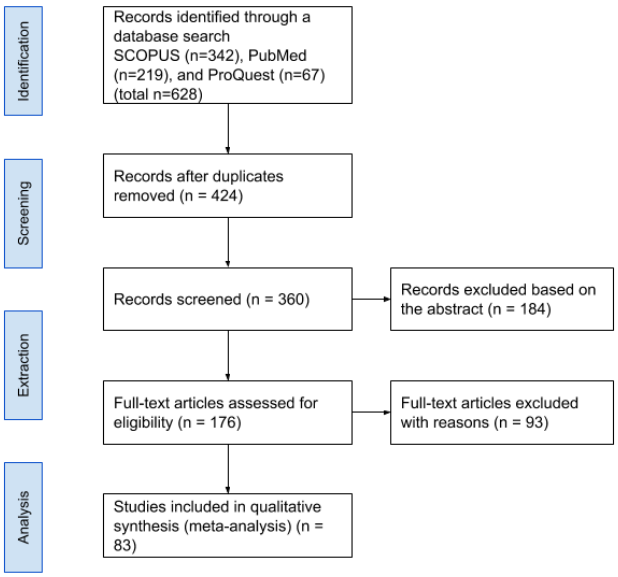

FIGURE 2. Flow diagram of the review process.

TABLE 1. Categories of studies in relation to the security and/or privacy of mHealth applications, including category overlaps.

Type of study	Subcategory	References
Evaluation techniques (n=44)	Security/privacy focus (n=26)	[1], [6], [8], [17], [22], [23], [27], [41], [51]–[68]
	General focus (n=18)	[2], [21], [24], [69]–[83]
Frameworks (n=10)	Evaluation frameworks (n=10)	[5], [64], [84]–[91]
Design recommendations and models (n=41)	Models (n=4)	[92]–[95]
	General recommendations that include S/P aspects (n=21)	[3], [4], [12], [76], [80], [81], [92], [96]–[110]
	S/P focused design features and recommendations (n=16)	[7], [25], [28], [51], [54], [57], [59], [66], [93]–[95], [111]–[114]

categorise them according to their primary contribution concerning the security and/or privacy of mHealth applications. This final corpus of 83 papers[7] had the following distribution: 44 studies are on mHealth app evaluation, 10 papers that reported on evaluation frameworks, and 37 papers that contained design recommendations and practices to ensure security and/or privacy of mHealth apps.[8] Table 1 shows the distribution of the included articles and the focus of their contributions.

Next, we discuss the health conditions covered in the included papers, followed by the privacy and security regulations that they refer to.

1) TARGET HEALTH CONDITIONS

The distribution of the health conditions targeted by included studies is depicted in Figure 3, which indicates that the majority of papers (45.9% or 39/83) addressed the security and privacy of general health and wellbeing (HWB) applications without considering specific health conditions. Interestingly, digital mental health interventions were the most addressed

[7]Some of the papers are included in multiple categories due to an overlap in contributions

[8]4 of those papers (4/37) were defined as models

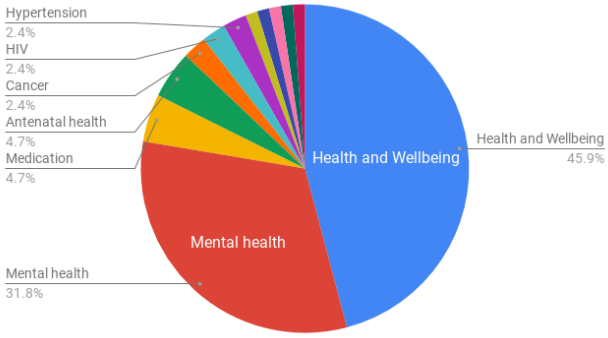

FIGURE 3. The distribution of addressed health conditions.

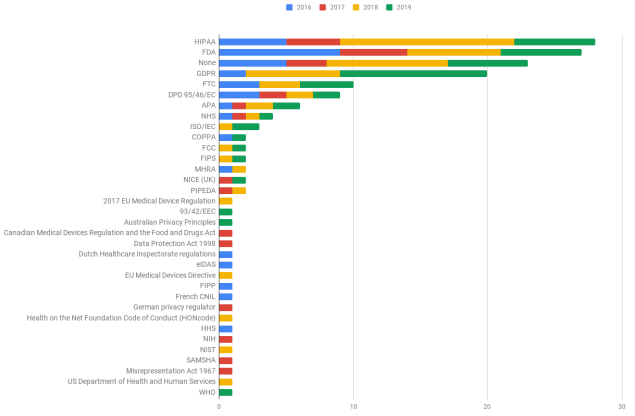

FIGURE 4. Regulations and regulatory bodies mentioned between April 2016 and August 2019.

when it comes to security and privacy (31.8% or 27/83), and 51.9% (14/27) of them focused on security and privacy specifically.[9] The presence of this large subset of the corpus motivated us to consider studies on digital mental health interventions in detail in Section V-D.

2) SECURITY AND PRIVACY REGULATIONS

As mentioned earlier, HIPAA and GDPR are among key regulations for the field of digital health interventions [115], which was reflected in the reviewed papers. It was found that 33.8% (28/83) of included papers mentioned HIPAA, 32.6% (27/83) referred to FDA, and 24.1% (20/83) mentioned GDPR. As an automatic search could overlook regulations and data protection laws that are less recognised, a manual check was performed to detect mentions of regulations.

Another relevant regulation is the Children's Online Privacy Protection Act (COPPA), a 1998 U.S. law that restricts operators of websites and online services from collecting the personal information of users under-13 without parental permission, which was mentioned only in 2.5% (2/83) of studies [97], [106].

Each country or region also has its own data protection laws, for instance, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada [62], [68] and Dutch Healthcare Inspectorate regulations [21]. However, 27.8% (23/83) of articles did not mention any data protection regulations and bodies at all.

Figure 4 shows the distribution of data protection regulations and regulatory bodies mentioned in the papers over the years: from April 2016 to August 2019.

Next, we address the first research question (RQ1): *What research-based evaluation frameworks and evaluation techniques are available to assess the security and privacy of mHealth applications?*

B. EVALUATION FRAMEWORKS FOR mHEALTH PRIVACY AND/OR SECURITY

12% (10/83) of all included papers presented their findings in the form of conceptual evaluation frameworks that were either focused on, or included, the process of privacy and/or security evaluation of mHealth applications.

Our analysis was based on the self-reported definition of findings as being "frameworks" in the included papers; all were found to be consistent with the definitions in Section III. None of the studies provided a definition of what comprises a security and privacy evaluation framework, they were instead presented by describing their goals and objectives, such as providing "the user with a strong tool to assist her decision on whether or not a given application found in some app store is trustworthy or not" [64, p.125] or "to establish a basis of safety, quality and effectiveness, in a way that assesses all relevant apps on an equal playing field" [88, p.1]. Nevertheless, in this study we follow the definition of a conceptual evaluation framework for mHealth as "a coherent set of actionable principles to protect patients' health information privacy" [46, p.3] (hereinafter "evaluation framework").

1) ORIGIN AND FOCUS

a: NEW EVALUATION FRAMEWORKS

Most of the papers in this category 70% (7/10) presented new frameworks developed by the study authors, and the methods adopted in their creation varied: from reviews of related literature and pre-existing app evaluation frameworks [84], [86], [89] to more empirical methods such as engaging an expert panel of key stakeholders [87] and analysis of mHealth applications [85].

Within this subset of studies, only 20% (2/7) of papers included a description of the application or validation of the suggested evaluation framework [64], [91]. In both cases this was performed by applying the frameworks to a set of mHealth applications.

b: EXISTING EVALUATION FRAMEWORKS

Three remaining studies applied existing frameworks to evaluate mHealth applications, which included "The Organisation for the Review of Care and Health Applications – 24 Question Assessment (ORCHA-24) framework" [88],

[9]Two papers targeting cognitive declines were also included

American Psychiatric Association (APA) App Evaluation Model and PsyberGuide[10] [5], and the GeoHealth Privacy Impact Assessment (PIA) framework [90].

Table 2 provides information on the validation of both new and existing evaluation frameworks.

c: EVALUATION FOCUS

This review does not consider each paper as a unit, but rather specific contributions, and attempts to make an explicit separation of the focus of those contributions. Only 40% (4/10) of frameworks were specific to the evaluation of security and/or privacy of mHealth applications. While one study focused solely on the privacy of mHealth apps by applying the Privacy Impact Assessment (PIA) framework [90], the remainder targeted both security and privacy at the same time.

Most of the studies in this category 60% (6/10) focused on overall evaluation of mHealth apps, including quality assessment [86], [89], review of official frameworks such as APA [5], and frameworks to support decision-making in choosing mHealth apps for research purposes [87].

Following the methodology proposed by [48] and based on the information provided in the included papers, we next describe the frameworks regarding the objectives of security and/or privacy evaluation, target stakeholders, and the phase of the mHealth app lifecycle the evaluation is suggested to be performed at.

2) "WHY", "WHEN", AND "WHO"

The frameworks identified had a variety of objectives for security and/or privacy evaluation, were suggested for different stages of mHealth app lifecycle, and are targeted for adoption by a range of different stakeholders. Based on the information extracted, we classified evaluation frameworks by three stages of the mHealth app lifecycle that they could be applied at: development, testing, and adoption or recommendation (Table 3)[11]

a: EARLY STAGE, DEVELOPMENT

Ensuring the security and privacy of sensitive medical data in health apps [85] or providing "a theoretical framework of rating criteria" that can be used to inform development of an evaluation tool for mHealth apps [86] were common objectives of the frameworks (Table 3, green colour). Target users here are app developers.

b: INTERMEDIATE STAGE, TESTING

At the intermediate stage between the creation of mHealth apps and their adoption (Table 3, yellow colour), studies address the following objectives: systematic identification and evaluation of potential privacy risks in mHealth Data Collection Systems [90], improving the quality of mHealth apps [91], and e-mental health assessment at organisational level or as a self-assessment for app developers [84]. Target users here are more mixed: app developers, health care providers, mental health advocates, app users, policy makers, and researchers.

c: FINAL STAGE, RECOMMENDATION AND ADOPTION

In the later stages, evaluation frameworks focus on questions such as what apps to adopt or recommend (Table 3, orange colour). The objectives of the evaluation may also differ depending on the target users. For app users: to provide the user with support for decisions on whether or not a given application found in an app store is trustworthy or not [64]. For researchers: a checklist for choosing digital health technologies for research [87]. For clinicians and healthcare professionals: to establish a sustainable curated app repository, based on explicit quality and risk criteria [89], to assist them with evaluating and integrating mental health apps into practice [5], and on what apps to recommend [88].

3) "WHAT" AND "HOW"

The summary of the conceptual evaluation frameworks presented in Table 2 includes information on the general evaluation objectives, evaluation methods, and validation of the presented frameworks.

Regarding evaluation of security and privacy, the frameworks can be broadly categorised in three groups: privacy factors, security factors, and contextual factors (related to the target users, intervention, or compliance of an app with standards and regulations). Table 3 illustrates the coverage of each of these groups by the frameworks, along with more fine-grained categories included in them.

Three types of evaluation techniques are suggested by the frameworks to reach these objectives. The first type is focused on app related evaluation, including evaluation of specific app features or functionality [85], [91].

Another perspective some of the frameworks adopt is user-focused evaluation. This includes evaluation of apps targeting specific user groups, for instance, adolescents [86] or people with mental health problems [84], or based on user input such as user reviews [64].

The final type of framework consists of checklists or sets of evaluation criteria or principles [5], [87]–[90]. More specifically, some of the frameworks go into more detail on evaluation suggestions and, in addition to more general objectives and principles, recommend evaluation tools and guidelines:

- "Interactive Mobile App Review Toolkit (IMART), "Evaluation methods in biomedical informatics", 2005";
- Tri-Council Guidelines regarding Ethical Conduct for Research Involving Humans;
- The Connected and Open Research Ethics (CORE) initiative;
- A Taxonomy of mHealth Apps–Security and Privacy Concerns.

[10]PsyberGuide (PsyberGuide.org) is a non-profit website reviewing smartphone applications and other digital mental health products.

[11]The ordering is compatibile with Table 2.

TABLE 2. Analysis of security/privacy conceptual evaluation frameworks (N = 10).

S/P focus	Framework	Evaluation objectives	Evaluation methods related to S/P	Validated?	Target stakeholders
Privacy	Privacy Impact Assessment (PIA) framework [90]	Potential privacy risks of mHealth Data Collection Systems	7 steps of privacy evaluation of the system: from a thorough consideration of the system and its adjacent infrastructure to identifying a complete list of threats and risks, and documenting them in a PIA report	yes	Community health workers
Security and privacy	Conceptual framework for the security of Android mHealth applications [85]	Security issues related to mHealth apps and Android system, and specific threats to mHealth apps	An empirical assessment of mHealth apps' security including their authentication, encryption, privacy, information leakage, suitability of requested data, etc	no	App developers
	A framework for testing security and privacy of mHealth apps [91]	Security and privacy of mHealth apps focusing on secure network connectivity and data transfer	Testing applications using static analysis of the source code and dynamic analysis of the runtime behavior, access to local services and storage as well as interaction with remote services with which the application communicates	yes	App developers
	Trust4App [64]	Trustworthiness health apps	Evaluation based on the following components of the automated framework: Data Collection Module, Rating Analyzer, Review Analyzer, S/P Quality Analyzer, Trust Module, and Trust Specification Module	yes	App users
	ORCHA-24 framework [88]	The quality of mHealth apps and identifying high-quality and low risk health apps in the absence of indicators such as National Health Service (NHS) approval	The assessment and ranking of apps is based on the three subsections of the ORCHA-24 review: data privacy, clinical efficacy and assurance, and user experience and engagement	yes	Clinicians
General evaluation including S/P components	Theoretical framework for evaluating the quality of mHealth apps for adolescent users [86]	The quality of mHealth apps targeted to adolescents	The evaluation is based on the following criteria: 1) Technical Quality, 2) Engagement, 3) Support System, 4) Autonomy, 5) Safety, Privacy, and Trust including the safety from social stigma, credibility, and information security	no	App developers
	E-mental health apps assessment framework in Canada [84]	Development of the guiding principles and assessment criteria of e-mental health applications	The assessment criteria include evaluation questions on transparency of information security and information security itself	no	App developers and users, health care providers, mental health advocates, policy makers, and researchers
	Digital research decision-making framework [87]	Development of guidance to facilitate responsible digital technology selection for research purposes	Evaluation based on the 4 decision-making domains and ethical principles: 1) Privacy, 2) Risks and Benefits, 3) Access and Usability, 4) Data Management, 5) Ethical Principles	no	Researchers
	Review of APA and PsyberGuide frameworks [5]	Review of the frameworks applicable to the identification of the potential privacy risks of mHealth Data Collection Systems	S/P evaluation steps of APA include Risk/Privacy and Security (Step 2), and the "Credibility, User Experience, Transparency" dimension in the PsyberGuide framework	yes	Clinicians and primary care professionals
	A common-sense app evaluation framework [89]	Supporting patients in choosing commonly available mHealth apps and potential to improve the quality of those applications	Evaluation based on the quality and risk criteria that should, for instance, identify apps of strategic interest to organisation, and low, medium, and high risk apps, in order to create a curated app collection	yes	Clinicians and professional societies

TABLE 3. Evaluation frameworks for different mHealth lifecycle points. Green: early stage, yellow: intermediate stage, orange: final stage.

Frameworks	Privacy related		Security related			Other		
	P/S policies	Permission requests	Data storage	Data transmissions	Vulnerability	Compliance	Intervention	User experience
[90]	X	-	-	X	X	-	-	X
[85]	X	X	X	X	X	-	-	-
[91]	-	-	-	X	X	-	-	-
[64]	-	X	-	-	-	-	-	X
[88]	X	-	-	X	X	-	X	-
[86]	X	-	-	-	X	-	-	X
[84]	X	-	-	-	-	-	-	-
[87]	X	-	-	X	X	X	-	X
PG [5]	X	-	-	-	-	-	-	-
APA [5]	X	-	X	X	X	X	-	X
[89]	X	-	-	X	-	-	-	-

Most of the reviewed frameworks present evaluation criteria as equally important, without capturing potential trade-offs and conflicts. However, 40% (4/10) of frameworks were presented as evaluation steps and hence did specify what aspects of a digital health intervention should have priority, capturing a hierarchy of evaluation criteria. For general mHealth evaluation, the American Psychiatric Association (APA) App Evaluation Model consists of sequential steps: from gathering background information to investigating the interoperability of the intervention, while "Risk/Privacy & Security" evaluation is recommended to be performed as early as on the step 2. Similarly, "data governance" evaluation is the first category of ORCHA-24 framework.

4) REPORTED FRAMEWORK LIMITATIONS

The papers on privacy and security evaluation frameworks also reported on the limitations of these frameworks. Some limitations concern the generalisability of findings, which could be due to specific healthcare settings and problem areas [5], patient populations included in the studies [86], or the categories of apps reviewed [88]. Another limitation is the uniform weighting that might be applied to mHealth evaluation. Furthermore, assumptions and judgments are based on the available information, which may be partial [88].

Other reported methodological limitations included a lack of stakeholder involvement that might result in missing important evaluation criteria and perspectives [90]. The findings not being complete and the need to update and refine them is another common limitation [87]. Many authors state that findings should not be seen as a replacement for more in-depth assessments, such as those using NHS digital assessment criteria, but rather as an adjunct [5], [87], [88].

C. SECURITY AND/OR PRIVACY EVALUATION TECHNIQUES

Studies that contained security and/or privacy evaluation techniques formed a majority of the included studies (53% or 44/83). Table 4 depicts the focus of evaluation reported by authors and evaluation categories that were extracted. 38.6% (17/44) of studies of this group focused on privacy of mHealth apps specifically, while security was covered only in 18.2% (8/44) of papers and only half of those studies (4/8) evaluated security of mHealth apps as their main focus. Another category (34.1% or 15/44) included a mix of security and privacy evaluation techniques where authors did not specify the evaluation focus and covered both dimensions at the same time.

TABLE 4. Categories of evaluation techniques in relation to the security and/or privacy of mHealth applications.

S/P focus	Evaluation focus	References
Privacy related	Among general app assessment criteria	5 studies [21], [70], [71], [77], [79]
	Permission evaluation	1 study [53]
	Privacy policy evaluation	5 studies [1], [23], [56], [58], [116]
	Trustworthiness evaluation	1 study [22]
	General privacy evaluation	5 studies [17], [27], [52], [55], [66]
	App quality evaluation	1 study [74]
Security related	Among general app assessment criteria	4 studies [2], [72], [78], [81]
	General security evaluation	2 studies [51], [57]
	Data storage analysis	2 studies [59], [67]
	Server side security evaluation	1 study [61]
Security and privacy evaluated together	Among general app assessment criteria	9 studies [24], [41], [69], [73], [75], [76], [80], [82], [83]
	General security and privacy evaluation focus	6 studies [6], [8], [54], [60], [62], [68]
Compliance	Both privacy and security aspects of the compliance	5 studies [2], [62], [63], [65], [82]

In addition to these categories, studies that included the evaluation of legal and regulatory compliance of mHealth

apps were coded, comprising 11.4% (5/44) of this subset, see the ''Compliance'' section in Table 4. These are considered separately due to the growing importance of compliance in the mHealth industry [65].

Next, we discuss the evaluation methods extracted from the included papers. As mentioned in Section III, we follow the taxonomy of Prat *et al.* [49]: the ''How'' of evaluation – noting the methods and tools used, the level of evaluation – and the ''What'' of evaluation, which includes the objectives or artefacts of evaluation, and the hierarchy of evaluation.

1) EVALUATION METHODS

The most common methodology was analysis of applications by downloading a sample of them or evaluating related information, e.g. user reviews or appstore descriptions, following certain evaluation criteria. Only one study did not evaluate applications or related information but focused on the development of an evaluation tool [82].

A major issue for app-software based evaluations is the effort and scale of the evaluation process. While the median number of evaluated apps was 53, their number varied for the types of the studies. Where apps were installed and evaluated manually, smaller numbers are typical. In other cases, where specific tools were used or aggregated data on apps was retrieved and analysed, numbers could be larger. For instance, the largest set of apps, 2133 wearable apps, was evaluated by Olabenjo and Makaroff [67]. The authors investigate and classify information leakage in Android wearable smartwatch apps, applying a scraper to collect various app characteristics, such as package name and Google Play link to the downloadable app which allowed them to download the Android Package (APK) files.

Similarly to the papers on evaluation frameworks, some of the studies presented evaluation techniques in a hierarchy of evaluation criteria. For instance, Marotta-Walters *et al.* present a guide with 9 app evaluation criteria, which starts from identifying a recommended user (''Does the app clearly state who should be using this app?'') to the appropriateness of use for other stakeholders (''Appropriate use: Is this app appropriate to be used by a clinician, client, or both?'') [70, p.7].

''Evaluators'' were considered as actors who performed the evaluation process or were involved in it, for instance, app users or healthcare professionals. In most cases, namely in 81.8% (36/44) of papers, evaluation of mHealth applications was performed only by researchers, i.e. authors of the articles. A smaller number of studies involved users and/or healthcare professionals in some way: clinicians participated in 13.6% (6/44) of studies and actively took part in the evaluation process in 4 of them, while app users or patients were involved in 6.8% (3/44) of studies. As for the involvement strategies, users or patients evaluated the user experience of mHealth apps [21], attended interviews and focus group discussions on their perspectives and experience of using them [72], or responded to a survey evaluating privacy policies (PPs) with the intention of making them more user-friendly [116]. As for healthcare professional involvement in research on privacy and security of mHealth, they were either included in app evaluation working groups, or acted as experts advising on the study design and implementation.

Only one paper reported on involving both patients and healthcare professionals, in a fully qualitative study on digital mental health interventions [72] where researchers and mental health professionals explored experiences and perspectives of aboriginal people in relation to their use of mental health apps.

Table 5 presents the categories and subcategories of the specific techniques provided in the selected papers including specific tools used (where applicable). These categories can be broadly defined as relating to:

- user or expert evaluation,
- content evaluation,
- technical security evaluation,
- functionality evaluation,
- compliance with security/privacy standards.

2) EVALUATION OBJECTIVES AND ARTEFACTS

During the data extraction phase, both the objectives of evaluation and specific app related artefacts were recorded and analysed. Common evaluation objectives and goals of the studies included research undertaken to support app stakeholders in selecting mHealth apps or identifying security and privacy issues from stakeholders' points of view. For instance, Parker *et al.* performed a content analysis of promotional (advertising) materials of mental health apps that are available to users at the point of choosing apps; their goal was ''to identify salient consumer issues related to privacy [...] to inform advocacy efforts towards promoting consumer interests'' [17, p.198].

Another common objective was to provide overviews of mHealth markets, comprising 27.3% (12/44) of papers. Such overviews were either based on the focus of the interventions, for instance, considering subsets of general health apps or apps specific to a certain health condition like pregnancy [77], or had specific evaluation goals. A good example of such goals is the study of Bondaronek *et al.* [75], which was undertaken to evaluate the quality of the most popular physical activity apps on the market using health care quality indicators.

Finally, evaluation of specific mHealth intervention components or app features was another commonly mentioned objective in investigating security and privacy. For instance, a study of Marotta-Walters *et al.* was designed to evaluate the benefits and risks of apps supporting a specific therapy – eye movement desensitization and reprocessing (EMDR) – when used by clients and/or clinicians [70]. 15.9% (7/44) of studies were undertaken to evaluate the data practices of mHealth applications, for instance, classification and analysis of information leakage in wearable smartwatch apps [67] or assessment of prominent transport security issues [57].

TABLE 5. Index of evaluation techniques.

Category	Subcategory	Specific tools or techniques	References
App content evaluation	Evaluation of the content provided by app developers (except PP and Terms of Agreement (ToA))	Healthcare expert evaluation [69], user evaluation [21], [72]	[2], [6], [8], [17], [21], [22], [24], [27], [41], [68]–[70], [72], [75], [77]–[79], [81]–[83]
	Privacy policy (PP) and Terms of Agreement (ToA) content evaluation	Readability assessment [17], [23], [56], [116]	[1], [6], [17], [22]–[24], [41], [55], [56], [58], [60], [68], [71], [74], [75], [77], [78], [83], [116]
Technical security mechanisms evaluation	Inspection of the code	Static analysis [54], [62], [65], [67], Dynamic code analysis [62], [65], [67], Vulnerability apps [51]	[51], [54], [62], [65], [67]
	Security transport issues tests	System for Semiautomatic Tests of Relevant Transport Security Issues [57], BProxy tool and Testssl script and the Qualys SSL Labs test suite [61], technical assessment of encrypted and unencrypted data transmission [55], analysis of the Bluetooth Low Energy protocol traffic [54]	[54], [55], [57], [61], [65]
Technical implementation evaluation	Functionality evaluation	Inform-Alert-Mitigate (I-AM) cycle analysis [66], data storage analysis [59], user evaluation [21], [72], App permission requests analysis [17], [53], [54]	[2], [17], [21], [27], [41], [53], [54], [59], [66], [68], [72]–[76], [81]–[83]
	Information leakage investigation	Scraper tool [67]	[67]
Compliance	Data Protection regulations compliance	Mixed methods: analysis of the privacy policies [63], compliance with Data Protection regulation requirements [62], server location [61]	[2], [62], [63], [65], [82]

On a more detailed level, Table 6 includes the categories and subcategories of evaluation artefacts and the numbers of papers that covered them.

3) "WHO" AND "WHEN"

In addition to evaluation objectives, the following aspects were coded: the stakeholders who would benefit from the suggested evaluation techniques, as defined by the authors, and the moment in the app lifecycle at which the evaluation should happen (level of evaluation). Similarly to the evaluation frameworks, most of the studies that suggested or applied various security and/or privacy evaluation techniques specified target mHealth stakeholders who could benefit or adopt them.

Studies that suggest or apply privacy and/or security evaluation techniques at the moment of app development (27.3% or 12/44) target: app developers and designers, app providers, and researchers. Evaluation of security and privacy at this stage included technical methods such as identifying transport security issues of the data flows [57], security vulnerabilities of mHealth apps [51], or evaluating content [82], functionalities [2], and legal compliance of the interventions [65].

Another category of evaluation technique was suggested to be applied at the stage when apps are already available to end users, comprising 56.8% (25/44) of papers. At this stage, almost all stakeholder groups were mentioned as a target audience, namely, patients and app users, clinicians and healthcare providers, app designers and developers, and data controllers. Examples of the evaluation methods here include studies of privacy in app user interfaces [66] and analysis of publicly available information in relation to the privacy and security of existing apps, such as privacy policies [1] or data handling information [60], [79].

Finally, the third category of studies are those that provide evaluation techniques targeted at the later stages in the app lifecycle (18.2% or 8/44): evaluations targeting clinicians to support them in recommending mHealth to their patients or direct evaluation by app users. Evaluation at this stage was mostly focused on the information available from app providers and app functionalities, for instance, to assess app quality [74], intervention relevance [76], [77], or privacy risks specifically [52].

D. SECURITY AND/OR PRIVACY DESIGN GUIDELINES

We next address the second research question and discuss the subset of included studies that produced design guidelines targeting the security and privacy of mHealth applications.

44.6% (37/83) of papers included design guidance, recommendations, and principles or reported on the design practices that were or could be used to ensure security and/or privacy of mHealth apps.

1) PRIVACY AND SECURITY CATEGORIES

Considering the complexity of the data extraction process, the final set of design recommendations resulted in roughly[12] 156 individual guidelines, which can be accessed in the supplementary materials.

As indicated in Section III, the categorisation process resulted in the final taxonomy depicted in Figure 1. The distribution of design guidance (Figure 5) within this taxonomy

[12]3 studies presented design recommendations graphically

TABLE 6. Evaluation artefacts related to security and privacy of mHealth apps.

Evaluation artefact	Subcategory	Num of papers	% to total (83)
App content and related information		52	62.7%
	Privacy policy and privacy related information		
	App vulnerability information		
	Installation information		
	App content		
	Marketing and promotional statements		
	App store ratings		
	Security information and measures		
	Consent		
	Intervention information		
	Data sharing information		
	Terms of service		
App functionality and design		31	37.4%
	App design		
	UX, UI, and usability		
	App characteristics		
	App functionalities		
App code		18	21.7%
	Code		
	App permission requests		
	Transmissions within and beyond the app		
	Data collection		
	Data storage		
	Data encryption		
User side		5	6.1%
	Authentication		
	Browsing data		
	Portability of personal data		
Compliance		5	6.1%
	GDPR compliance		
	HIPAA compliance		
	Legal and ethical compliance		

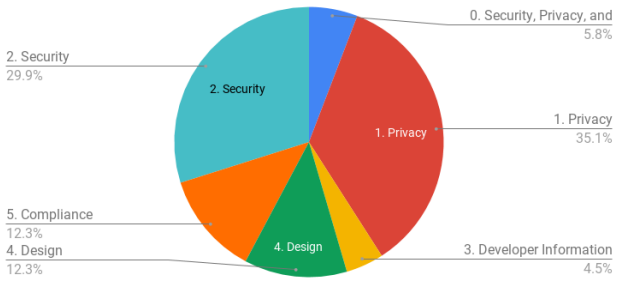

FIGURE 5. Distribution of design guidelines.

indicates that privacy of mHealth apps and factors included in it, for instance, data ownership, were covered by a larger number of individual guidelines than those targeting app security.

While privacy was the largest category among the guidelines (35.1% of all guidelines), security-focused guidelines (roughly 29.9% of all design recommendations) included such topics as secured data transfer, storage, and user authentication.

2) ORIGIN OF DESIGN GUIDELINES

As mentioned in Section III, the methods used to generate design guidelines were coded at the extraction phase, which resulted in three main sources of design contributions: syntheses of related literature or regulations, user studies involving patients or mHealth app users and healthcare professionals, and empirical studies. We next discuss each of these in more detail.

Literature and regulation reviews were conducted by 24.3% (9/37) of studies that produced security and privacy design guidance. Most of the reviews covered previous research relevant to security and privacy of mHealth interventions, with the focus either on general literature on mHealth or on specific topics related to it. For instance, Thach [80] summarises the literature on user reviews of Cognitive Behavioural Therapy (CBT) apps in order to identify

reasons for low adherence, and Naeem *et al.* [101] review the literature on adverse effects of mental health apps in order to provide recommendations on how to overcome them. Other reviews analysed policies, regulations, and standards related to security and privacy of digital health. For instance, Parker *et al.* [28] conducted a review of policies produced by governments and non-government organisations in Canada for mental health apps in order to identify relevant sectors, policy actors, and policy solutions.

Among the reviews, two studies reviewed app functionalities or possible adverse effects of health apps. For instance, the only systematic literature review targeted pregnancy monitoring apps [81], the components that are normally included in them (e.g. diaries or backup), and their quality assessment metrics.

User generated recommendations came from studies involving patients and app users with either specific health conditions or a general interest in mHealth. They comprised 32.4% (12/37) of papers in this group. The most common methodologies applied in such studies were focus group discussions, interviews, and surveys. Two studies provided guidelines based on co-design sessions that included e-Health experts, clinicians, and cancer survivors [3] or HIV patients [99].

This category also included two studies that modelled user intentions to disclose personal health information, including factors related to privacy concerns [92], or privacy preferences [93].

The third category of studies produced design guidelines or recommendations arising from **empirical studies**, comprising 40.5% (15/37) of papers in this group. The design contributions were either the result of analysis of existing apps or their components, or app development studies without user involvement. Examples of such studies include the analysis and development of secure data sharing mechanisms [59], which differ from the user generated contributions discussed above.

40% (6/15) of these studies reviewed the components or characteristics of existing apps, resulting in new security and privacy recommendations. Another type of study in this category (53.3% or 8/15) – app development – included security and privacy design contributions which were produced from applications targeting various types of health conditions. These included cancer [105], multiple sclerosis [108], and mental health difficulties [107]. All but one of these papers also conducted an evaluation study of the app they developed: either in the form of a user acceptance study [105], [108] or by applying technical analysis techniques, such as security (active and passive attacker) or performance analysis [95].

3) FORM OF GUIDANCE

The guideline extraction process showed two general trends. While some of the studies clearly presented sets of design recommendations, for other papers, identifying and extracting guidelines required much more effort and time, as guidelines were presented as experiment outcomes, future recommendations, and observations. We identified *3 categories of design contributions*: 1) clearly presented guidelines, recommendations, or principles; 2) app development practices including applied security and privacy mechanisms and tools to ensure mHealth security and/or privacy; 3) models of user behaviour and preferences related to security and/or privacy.

Design contributions in the form of design **guidelines and principles** were reported by 35% (13/37) of papers in this category. While some of them targeted security and privacy specifically [7], [51], [59], others were a part of more general sets of recommendations targeting the field of mHealth.

Another distinct topic covered by those guidelines related to security and privacy is the transparency of data handling by mHealth apps. An example is the study of Wykes *et al.* which proposes design principles that responsible Health App Marketplaces should follow [25]. There were also guides that were focused on issues related to the design of secure and private mHealth interventions. For instance, two studies provided ethical guidelines based on reviews of relevant literature, regulations, and standards [12], [100], which are intended to be taken into consideration in the development and evaluation of mental health apps.

Another study by Turner-McGrievy *et al.* provides a guide intended to support researchers in choosing the mode of delivery for mobile behavioral interventions [97], which includes data security and consumer privacy requirements that should be considered in this process.

The rest of the recommendations came in the form of developer's guides or design recommendations applicable to the mHealth app development process in general. As research-based best practices for building apps can help developers to avoid mistakes throughout this process, we identified the next category of design contributions as **"development practices"**. For instance, in their study Lang *et al.* describe the practices they adopted for ensuring data security in the development of an app for multiple sclerosis patients [108]. Another example of this form of design contribution is the description of the steps taken to design an Arabic weight-loss app that considers user privacy and data security by applying a number of guidelines and procedures [109].

10.8% (4/37) of studies presented their contribution in the form of **models** of app users' behaviour. They included a model of intentions to disclose personal health information, including factors related to privacy concerns [92], and a model of users' privacy preferences [93]. Another study developed the "Privacy Model for Mobile Data Collection Applications" (PM-MoDaC) for apps related to the collection of mobile data for tracking daily routines, which includes 9 privacy mechanisms to ensure privacy: from user consent to secure data transfer [94]. Finally, Greene *et al.* report on three security models that could be applied to the sharing of mHealth data streams, namely the adversary model, threat model, and trust model [95].

V. DISCUSSION

This section presents a discussion of the results arising from this scoping review, including the topics that emerged from the qualitative analysis, and the implications of these results.

The goal of this literature review was twofold: to provide an overview and synthesis of research studies that evaluate security and privacy of mHealth applications (RQ1) and to review research-based design recommendations for ensuring them (RQ2).

The last four years of research on security and privacy of mHealth apps have seen a wide variety of contributions that target a range of digital health services. The works included in this review address critical questions related to increasing the security and privacy of health apps. They do this by evaluating existing apps and providing design recommendations for new ones. However, the analysis has uncovered shortcomings and gaps in the literature related to the topics of regulation compliance, uneven coverage of health conditions, evaluation techniques, design guidelines, and accessibility and reliability of findings. We discuss those issues below.

Over a third of included papers considered privacy and security together, as a part of a general evaluation of mHealth design. Security and privacy might overlap – for instance, in ensuring patients' confidentiality – however, these two dimensions have fundamental differences: while security relates to **protection** against unauthorized access to data, privacy is an individual's right to **maintain control** over and be free from intrusion into their private data and communications, and relates to **trust** in mHealth services. Moreover, an exclusive focus on security can increase surveillance and data collection, which introduces potential privacy risks. Unsurprisingly, the methods to evaluate these two dimensions differ as well: methods for security may place more emphasis on technical evaluation while methods for privacy may be more user oriented.

Besides security and privacy of mHealth data, some of the studies raised the issue of safety, namely, safety from social stigma, and mHealth intervention safety for end-users. Other studies have raised the issue of third-party services as potential threats to safety [8]. Another topic mentioned in passing was evaluation of ethics of mHealth interventions, and how ethical issues might be addressed. While both of these topics are relevant and important to digital health interventions, the lack of discussion of them within the papers was a notable omission.

A. REGULATIONS AND COMPLIANCE

MHealth services, including health apps, digital therapeutics, and ''software as a medical device'' have to comply with regulations at both a national and international level. However, few studies mentioned and fewer still focused on compliance with existing regulations in their evaluations and design recommendations.

Nevertheless, much of the research within the corpus addresses both security and privacy mechanisms, and specific components within digital health interventions that contribute to compliance. For instance, such components include the data flows, support of users' data ownership, and audit of collection of specific data types over time. These factors contribute towards the paradigm of privacy and security by design; required by GDPR in the EU, but also recognised and endorsed by other regulatory authorities worldwide. This research trend is especially important as a ''compliance-focused'' style still prevails, which reduces the focus on privacy and user needs within the design process [18].

To address this need, we would advocate for a repository of evaluation methods and design guidelines that would support compliance but also provide a fine-grained view on incorporating security and privacy for digital health into the design process. Such a resource would support app designers and healthcare professionals, as they have specific security and privacy-related needs and requirements to fulfil that go beyond those that typically apply in research studies.

B. EVALUATION TECHNIQUES

Studies focused on security and privacy evaluation included various methods and frameworks, proposing evaluation techniques that could be broadly categorised as technical and non-technical (heuristic).

1) TECHNICAL EVALUATION

Technical evaluations included techniques such as static analysis to highlight app vulnerabilities by examining code or traffic analysis during simulated use to detect potential data leaks or security measures taken during transmission. These techniques were applied in empirical studies that generally consisted of downloading apps and inspecting the software. While these studies demonstrate the process of application and use of these technical evaluation techniques, limitations include their specificity and the difficulty of generalising and applying them to different contexts. For instance, some of them are specific to the type of mHealth intervention, such as Eye Movement Desensitization and Reprocessing (EMDR) [70] or medication use apps [21], or evaluate the security or privacy of apps with specific features, for instance, analysing the traffic between a fitness tracker and a smartphone app [54].

Most of the evaluated apps were *free*, which could be justified by their popularity among the users and easier access by the researchers. However, this fact also illustrates potential failures in transparency or auditability of app behaviours and keeps a large area of paid apps untapped by research. Previous research recognises users' perception of better data protection and privacy within paid services - the ''paying for privacy'' misconception [117] - which has received considerable criticism. Hence, more work is needed in reviewing paid apps as well.

There were also more general evaluation objectives such as app usability or app functionality that contributed to security and privacy recommendations for future research. For instance, analysis from the perspective of function usefulness [76] or mHealth intervention features,

such as pain diary function [81], may lead to observations regarding poor security mechanisms or missing regulatory compliance.

2) HEURISTIC EVALUATION

Non-technical or heuristic evaluation techniques consisted of evaluation of information provided by app producers, user studies with various mHealth stakeholders, and literature reviews.

Evaluation of self-declared data from app developers was the most common privacy assessment technique. These studies focused on privacy policies, terms of agreement, and informed consent by analysing the availability and readability of these disclaimers or comparing them to the **marketing statements** of app providers, in order to determine whether they are consistent with each other, with the regulations, and with the expectations of users. However, no studies addressed the dynamic nature of such documentation and the techniques to support it by design. Moreover, the granular personal data generated by mHealth, and privacy policies that are already too complex to read but that keep getting longer over time, weaken user privacy on the internet [118], an issue that is important to address for digital health interventions. While lean methods categorized under the umbrella term 'agile' might not always apply to digital health, one of its core principles – ''customer collaboration over contract negotiation'' [119] – could be beneficial for motivating users' trust. Researchers in mHealth must advocate for user-centered privacy and informed consent practices to proactively maintain transparency and protect the interests of mHealth users.

A related issue concerns the need for ''dynamic consent'' when applications are used (possibly intermittently) over the longer term. For instance, when new data types or processing capabilities are added, or where apps are deleted and re-installed.

Evaluation based on app **user reviews** was another way of extracting evidence on app security and privacy. Positive and negative reviews trigger different reactions and are perceived differently - a phenomenon called ''negative bias'' such that more negative reviews are more influential than positive reviews [120], a finding which has been confirmed repeatedly by researchers in many social science disciplines. More recent studies have looked deeper into this issue; for instance, a study by Wu provides evidence that the valence of online reviews is positively associated with their helpfulness, explaining that ''satisfied customers are motivated to write well-composed and in-depth reviews, while unhappy customers provide less transferable information'' [121, p.997]. As there is an increasing market for fake positive online reviews [122], evaluation methods based on user reviews do not seem reliable as a sole indicator for assessing the security or privacy of mHealth applications.

While most of the studies were categorised into one of the three groups of evaluation frameworks, evaluation techniques, and design recommendation and practices, several papers included *cross-category contributions*, such as cases where evaluation techniques are followed by design guidelines to improve the security and privacy of mHealth apps. These included evaluation of security vulnerabilities of mHealth applications [51], transport issues [57], or evaluation of specific security mechanisms like ''secure data container'' [59], that were followed by security assurance recommendations.

C. DESIGN RECOMMENDATIONS

Previous research acknowledges that the identification of guidelines and the effort necessary to recognize and extract them from each selected paper highly depends on the way they are presented, as well as the skills of experts in identifying them [123]. As we discovered at the stage of qualitative analysis, the guideline extraction process was not always straightforward. Only one third of the studies presented their design contributions in the form of guidelines or instructions to improve the security and privacy of mHealth apps, which were easy to extract, interpret, and categorise.

Other forms of guidance included development practices – descriptions of the application of security or privacy mechanisms – and models, e.g. predictions or simulations of user behaviour or preferences. For these categories of papers, guideline identification and extraction required more effort and time, as guidelines were presented as experiment outcomes, future recommendations, and observations.

Our literature review included other types of studies that included design guidance, such as studies drawing on user perspectives to provide recommendations [80] and review papers that analysed the literature on regulations, and previously identified security and privacy issues, in order to provide recommendations [54].

While more than half of the included studies mentioned mHealth developers and designers as their target audience, making findings and contributions difficult to identify and consume acts as a barrier to the uptake of recommendations. The use of standard formats for reporting, and the development of knowledge bases could help address this issue and benefit the wider community.

The application of design guidelines was described in only five papers, which provided design recommendations to be applied during the process of app development, and conducted evaluation studies to validate their findings [95], [105], [107]–[109]. While this process supports the usability and a certain degree of reliability of findings, a greater number of independent studies is needed to validate evaluation methods and guidelines.

D. DIGITAL MENTAL HEALTH INTERVENTIONS

Mental health was the domain most commonly addressed by the studies included in the review (Figure 3). The motivation to examine the security of privacy of mental health apps can be viewed broadly in terms of *risks and opportunities*. Regarding the risks, researchers agree that by using mHealth apps, people with cognitive decline and mental health difficulties are potentially exposed to privacy breaches. Their data

should be protected [58] and privacy policies should be easily understandable and should not prevent users from making informed decisions [23].

Nevertheless, the potential of mental health apps to benefit users is perceived as being high. They can support users in many ways: by increasing users' understanding of their conditions [24], by increasing end-user adherence to interventions [80], and even by complementing or replacing face-to-face therapy when appropriate [110]. However, previous research also agrees that the acceptance of such interventions should be carefully evaluated [72].

Studies covered a wide range of *mental health conditions*, which included stress [3], depression [55], [60], [71], sleep disorders [88], smoking cessation [55], [98], psychosis [4], anxiety [53], and cognitive decline such as dementia [58], [65]. Studies also addressed specific *mental health interventions*, such as cognitive behavioural therapy (CBT) or behavioural activation (BA) for depression [71] and behaviour change [41], eye movement desensitization and reprocessing (EMDR) [70], and mood tracking [56].

Several studies on mental health apps have been conducted with patients having conditions such as cancer or trauma comorbidities, which indicates that mental health is relevant to patients across a range of health conditions. For instance, patients with heart failure or other chronic conditions often experience mental health difficulties [3].

Most of the studies on evaluation of mental health apps focused on privacy, emphasising that privacy concerns might prevent patients from using mental health apps and, moreover, might negatively impact the intervention itself [17]. Critical evaluation of apps' privacy is seen as a key consideration in the design of such therapeutic tools [56], for instance, by applying a specific framework [84] to evaluate digital mental health applications or adopting existing evaluation frameworks such as the American Psychiatric Association (APA) App Evaluation Model, PsyberGuide [5], or Organisation for the Review of Care and Health Applications (ORCHA-24) [88].

Design recommendations to ensure security and privacy of mental health apps were obtained as a result of literature reviews, user studies, and empirical studies on evaluation of existing mental health apps. However, most of these studies did not report on the application of the suggested recommendations, and further work on validation of such recommendations is clearly required.

E. LIMITATIONS

The nature of the search terms may have limited the review results. The search terms could have been modified to include words such as 'medical apps' or 'medical devices', which would likely have captured more work, at the cost of introducing many more non-relevant papers to the screening process. This work focused on the term 'health apps' because of the scalability of distribution for mobile apps. Still, in doing so, it may have missed relevant material regarding the security and privacy of other categories of mHealth interventions. Another limitation of this work is the necessity of choosing a time interval for the works included in the review. The interval was chosen to reflect research published since GDPR was approved in 2016 but, as with any date restriction, this risks excluding potentially relevant work.

One further limitation is related to the extraction and categorisation process of guidelines from papers where they were not presented as such, as this can be seen as having a greater subjective element, and so in the extraction spreadsheet (supplementary materials), guidelines that were not presented as such by the original authors are marked as such.

VI. CONCLUSIONS AND FUTURE WORK

We have presented a scoping review, based on a systematic search, which identified research trends on the topics of security and privacy evaluation and design for mHealth applications. The evaluation frameworks, techniques, tools, and design guidelines extracted from the literature provide a knowledge base, which can be consulted and applied when developing mHealth applications that seek to safeguard the security and privacy of users' sensitive data. More specifically, we identified the critical moments of the mHealth app lifecycle at which specific evaluation techniques could be applied: from the design and creation of an app to the testing and finally, adoption and recommendation to patients. A promising direction for future research could focus on embedding those tools further into the digital health development process to facilitate ''privacy by design'' principles and bring development and design teams closer to compliance with regulatory frameworks.

Despite increasing awareness and research activity addressing the security and privacy of digital health interventions in recent years, there are still substantial gaps in the field. Further work is needed on improving the reporting and characterization of research-derived evaluation techniques and guidelines. It is also clear that a community effort towards validating and reproducing findings will help in providing more solid and actionable research guidelines. Moreover, the distinctions between security, privacy and related concepts such as data protection should be emphasised, recognising the different approaches to ensuring them in mHealth. Furthermore, the related topics of ethics and safety should also be taken into account when evaluating mHealth apps and suggesting design recommendations.

Only a few studies involved mHealth users and healthcare professionals in the evaluation of mHealth interventions, which is another current research shortcoming and an opportunity for future studies.

APPENDIX A
STUDIES THAT PRODUCED DESIGN GUIDELINES

See Table 7.

TABLE 7. Studies that provided mHealth security and privacy design recommendations.

N	Paper	Pub year	Form of guidance	Type of study
1	"Attitude" - mHealth apps and users' insights: An empirical approach to understand the antecedents of attitudes towards mHealth applications [96]	2019	Guidelines	User studies
2	A health app developer's guide to law and policy: a multi-sector policy analysis [28]	2017	App developer's guide	Literature review
3	A Mobile App for Assisting Users to Make Informed Selections in Security Settings for Protecting Personal Health Data: Development and Feasibility Study [113]	2018	Security features	User studies
4	A realistic talking human embodied agent mobile phone intervention to promote HIV medication adherence and retention in care in young HIV-positive African American men who have sex with men: Qualitative study [103]	2018	App features	User studies
5	A Stress Management App Intervention for Cancer Survivors: Design, Development, and Usability Testing [3]	2018	Security and privacy considerations	User studies
6	A vulnerability study of Mhealth chronic disease management (CDM) applications (apps) [51]	2018	Security recommendations	Empirical study
7	Are mHealth Apps Secure? A Case Study [54]	2018	Data protection requirements and practices in mHealth apps	Literature review
8	Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study [111]	2019	Security and privacy features	User studies
9	Can Your Phone Be Your Therapist? Young People's Ethical Perspectives on the Use of Fully Automated Conversational Agents (Chatbots) in Mental Health Support [110]	2019	Ethical standards	User studies
10	Chinese Mobile Health APPs for Hypertension Management: A Systematic Evaluation of Usefulness [76]	2018	Design recommendations	Empirical study
11	Choosing between responsive-design websites versus mobile apps for your mobile behavioral intervention: presenting four case studies [97]	2016	Guide for researchers	Empirical study
12	Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues [57]	2017	Design practices for mHealth transport issues	Empirical study
13	Co-Design of a Consultation Audio-Recording Mobile App for People With Cancer: The SecondEars App [105]	2019	App design	Empirical study
14	Design Considerations for mHealth Programs Targeting Smokers Not Yet Ready to Quit: Results of a Sequential Mixed-Methods Study [98]	2017	mHealth intervention features	User studies
15	Development of an mHealth platform for HIV care: Gathering user perspectives through co-design workshops and interviews [99]	2018	Users' views	User studies
16	Development of Usability Guidelines for Mobile Health Applications [106]	2019	Design guidelines	User studies
17	Ethical guidelines for mobile app development within health and mental health fields [100]	2016	Ethical guidelines	Literature review
18	Ethical Issues for Direct-to-Consumer Digital Psychotherapy Apps: Addressing Accountability, Data Protection, and Consent [12]	2018	Ethical guidelines	Literature review
19	Evaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study [104]	2018	mHealth app development practices	User studies
20	Feasibility and Acceptability of Using a Mobile Phone App for Characterizing Auditory Verbal Hallucinations in Adolescents With Early-Onset Psychosis: Exploratory Study [4]	2019	Users' views	User studies

TABLE 7. *(Continued.)* **Studies that provided mHealth security and privacy design recommendations.**

21	Mobile personal health records for pregnancy monitoring functionalities: Analysis and potential [81]	2016	Design recommendations	Literature review
22	PatientConcept App: Key Characteristics, Implementation, and its Potential Benefit [108]	2019	App development	Empirical study
23	Poster: Design ideas for privacy-aware user interfaces for mobile devices [66]	2016	Privacy design ideas	Empirical study
24	Reporting and understanding the safety and adverse effect profile of mobile apps for psychosocial interventions: An update [101]	2016	Design practices	Literature review
25	Secure sharing of mHealth data streams through cryptographically-enforced access control [95]	2019	Security features	Empirical study
26	Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide [7]	2016	Security guide	Empirical study
27	The Development of an Arabic Weight-Loss App Akser Waznk: Qualitative Results [109]	2019	App development	Empirical study
28	The Effortless Assessment of Risk States (EARS) Tool: An Interpersonal Approach to Mobile Sensing [107]	2018	App development	Empirical study
29	The secure data container: An approach to harmonize data sharing with information security [59]	2016	Security recommendations	Empirical study
30	Tracing personal data using comics [114]	2017	App development	Empirical study
31	Translating GDPR into the mHealth Practice [112]	2018	GDPR compliance recommendations	Literature review
32	User's perception on mental health applications: A qualitative analysis of user reviews [80]	2018	Design features	Literature review
33	What Is Being Used and Who Is Using It: Barriers to the Adoption of Smartphone Patient Experience Surveys [102]	2019	Design recommendations	User studies
34	Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces [25]	2019	Design principles	Literature review
35	Context Data Categories and Privacy Model for Mobile Data Collection Apps [94]	2018	Privacy design recommendations	Empirical study
36	A Model to Protect Sharing Sensitive Information in Smart Watches [93]	2017	Model, UI design	Empirical study
37	Determinants of Personal Health Information Disclosure: A Case of Mobile Application [92]	2018	Model	User studies

APPENDIX B
SEARCH QUERIES

1) ProQuest

ab(health OR mental health) AND ab(app OR apps) AND ab(security OR privacy) since 1/04/2016 – 137 results

2) PubMed

((mental health[Title/Abstract] OR health[Title/Abstract]) AND (app[Title/Abstract] OR apps[Title/Abstract])) AND (security[Title/Abstract] OR privacy[Title/Abstract]) AND (''2016/04/01''[PDAT]: ''2019/08/06''[PDAT]) – 219 results

3) SCOPUS

(ABS (security OR privacy) AND ABS (apps OR app) AND ABS (health OR (mental AND health))) AND (LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) OR LIMIT-TO (PUBYEAR, 2017) OR LIMIT-TO (PUBYEAR, 2016)) AND (LIMIT-TO (LANGUAGE, ''English'')) – 345 results

REFERENCES

[1] M. Bachiri, A. Idri, J. L. Fernández-Alemán, and A. Toval, ''Evaluating the privacy policies of mobile personal health records for pregnancy monitoring,'' *J. Med. Syst.*, vol. 42, no. 8, p. 144, Jun. 2018, doi: 10.1007/s10916-018-1002-x.

[2] P. Zhao, I. Yoo, R. Lancey, and E. Varghese, ''Mobile applications for pain management: An app analysis for clinical usage,'' *BMC Med. Informat. Decis. Making*, vol. 19, no. 1, p. 106, Dec. 2019.

[3] E. Børøsund, J. Mirkovic, M. M. Clark, S. L. Ehlers, M. A. Andrykowski, A. Bergland, M. Westeng, and L. S. Nes, ''A stress management app intervention for cancer survivors: Design, development, and usability testing,'' *JMIR Formative Res.*, vol. 2, no. 2, p. e19, Sep. 2018.

[4] R. E. Smelror, J. J. Bless, K. Hugdahl, and I. Agartz, ''Feasibility and acceptability of using a mobile phone app for characterizing auditory verbal hallucinations in adolescents with early-onset psychosis: Exploratory study,'' *JMIR Formative Res.*, vol. 3, no. 2, May 2019, Art. no. e13882. [Online]. Available: http://europepmc.org/articles/PMC6537505

[5] J. C. Magee, S. Adut, K. Brazill, and S. Warnick, ''Mobile app tools for identifying and managing mental health disorders in primary care,'' *Current Treatment Options Psychiatry*, vol. 5, no. 3, pp. 345–362, Sep. 2018.

[6] B. H. Sampat and B. Prabhakar, "Privacy risks and security threats in mHealth apps," *J. Int. Technol. Inf. Manage.*, vol. 26, no. 4, pp. 126–153, 2017.
[7] E. P. Morera, I. de la Torre Díez, B. Garcia-Zapirain, M. López-Coronado, and J. Arambarri, "Security recommendations for mHealth apps: Elaboration of a developer's guide," *J. Med. Syst.*, vol. 40, no. 6, p. 152, 2016.
[8] Q. Grundy, F. P. Held, and L. A. Bero, "Tracing the potential flow of consumer data: A network analysis of prominent health and fitness apps," *J. Med. Internet Res.*, vol. 19, no. 6, p. e233, Jun. 2017.
[9] Q. Grundy, K. Chiu, F. Held, A. Continella, L. Bero, and R. Holz, "Data sharing practices of medicines related apps and the mobile ecosystem: Traffic, content, and network analysis," *BMJ*, vol. 364, no. l920, p. 1, 2019.
[10] D. Kotz, "A threat taxonomy for mHealth privacy," in *Proc. 3rd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2011, pp. 1–6.
[11] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Hum. Rights Law Rev.*, vol. 14, no. 3, pp. 441–458, Sep. 2014.
[12] N. Martinez-Martin and K. Kreitmair, "Ethical issues for direct-to-consumer digital psychotherapy apps: Addressing accountability, data protection, and consent," *JMIR Mental Health*, vol. 5, no. 2, p. e32, Apr. 2018.
[13] *Standards for Privacy of Individually Identifiable Health Information. Final Rule, 45 CFR Parts 160, and 164. Code of Federal Regulations*, United States Dept. Health, Hum. Services, Washington, DC, USA, 2010.
[14] C. Arora, "Digital health fiduciaries: Protecting user privacy when sharing health data," *Ethics Inf. Technol.*, vol. 21, pp. 181–196, Feb. 2019.
[15] L. Savage, M. Gaynor, and J. Adler-Milstein, "Digital health data and information sharing: A new frontier for health care competition?" *Antitrust Law J.*, vol. 82, no. 2, pp. 593–621, 2019.
[16] (Feb. 2020). *Eu Data Protection Rules*. [Online]. Available: https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en
[17] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices," *Int. J. Law Psychiatry*, vol. 64, pp. 198–204, May 2019.
[18] A. E. Waldman, "Designing without privacy," *Houston Law Rev.*, vol. 55, p. 659, Feb. 2018.
[19] C. A. Tschider, "The consent myth: Improving choice for patients of the future," *Washington Univ. Law Rev.*, vol. 96, no. 6, p. 1505, 2018.
[20] J. C. Wyatt, H. Thimbleby, P. Rastall, J. Hoogewerf, D. Wooldridge, and J. Williams, "What makes a good clinical app? Introducing the RCP health informatics unit checklist," *Clin. Med.*, vol. 15, no. 6, pp. 519–521, Dec. 2015.
[21] L. W. M. van Kerkhof, C. W. E. van der Laar, C. de Jong, M. Weda, and I. Hegger, "Characterization of apps and other e-tools for medication use: Insights into possible benefits and risks," *JMIR mHealth uHealth*, vol. 4, no. 2, p. e34, Apr. 2016.
[22] K. M. Scott, D. Richards, and G. Londos, "Assessment criteria for parents to determine the trustworthiness of maternal and child health apps: A pilot study," *Health Technol.*, vol. 8, nos. 1–2, pp. 63–70, May 2018.
[23] A. Powell, P. Singh, and J. Torous, "The complexity of mental health app privacy policies: A potential barrier to privacy," *JMIR mHealth uHealth*, vol. 6, no. 7, p. e158, Jul. 2018.
[24] A. Radovic, P. L. Vona, A. M. Santostefano, S. Ciaravino, E. Miller, and B. D. Stein, "Smartphone applications for mental health," *Cyberpsychol., Behav., Social Netw.*, vol. 19, no. 7, pp. 465–470, Jul. 2016.
[25] T. Wykes and S. Schueller, "Why reviewing apps is not enough: Transparency for trust (T4T) principles of responsible health app marketplaces," *J. Med. Internet Res.*, vol. 21, no. 5, May 2019, Art. no. e12390.
[26] K. Huckvale, J. T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car, "Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment," *BMC Med.*, vol. 13, no. 1, p. 214, Dec. 2015.
[27] L. Hutton, B. A. Price, R. Kelly, C. McCormick, A. K. Bandara, T. Hatzakis, M. Meadows, and B. Nuseibeh, "Assessing the privacy of mHealth apps for self-tracking: Heuristic evaluation approach," *JMIR mHealth uHealth*, vol. 6, no. 10, p. e185, Oct. 2018.
[28] L. Parker, T. Karliychuk, D. Gillies, B. Mintzes, M. Raven, and Q. Grundy, "A health app developer's guide to law and policy: A multi-sector policy analysis," *BMC Med. Informat. Decis. Making*, vol. 17, no. 1, p. 141, Dec. 2017.
[29] *Children's Online Privacy Protection Rule ('Coppa')*, Federal Trade Commission, Washington, DC, USA, Sep. 2016, vol. 29.
[30] R. Zuraw and T. Sklar, "Digital health privacy and age: Quality and safety improvement in long-term-care," *Indiana Health Law Rev.*, vol. 17, p. 85, Mar. 2020.
[31] U.S. Food and Drug Administration. *Medical Devices, X STOP Interspinous Process Decompression System (XSTOP)–P040001*. Accessed: Sep. 20, 2014. [Online]. Available: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/Recently-ApprovedDevices/ucm078378.htm
[32] C. Sorenson and M. Drummond, "Improving medical device regulation: The United States and Europe in perspective," *Milbank Quart.*, vol. 92, no. 1, pp. 114–150, Mar. 2014.
[33] U.-V. Albrecht, O. Pramann, and U. von Jan, "Medical apps—The road to trust," *Eur. J. Biomed. Informat.*, vol. 11, no. 3, pp. en7–en12, 2015.
[34] T. J. Kasperbauer and D. E. Wright, "Expanded FDA regulation of health and wellness apps," *Bioethics*, vol. 34, no. 3, pp. 235–241, Mar. 2020.
[35] S. Katuu and M. Ngoepe, "Managing digital records within South Africa's legislative and regulatory framework," in *Proc. 3rd Int. Conf. Cloud Secur. Manage. (ICCSM)*, 2015, pp. 59–70.
[36] S. Gurses and J. V. J. van Hoboken, "Privacy after the agile turn," *SocArXiv*, May 2017, doi: 10.31235/osf.io/9gy73.
[37] S. Khan and A. S. M. L. Hoque, "Digital health data: A comprehensive review of privacy and security risks and some recommendations," *Comput. Sci. J. Moldova*, vol. 24, no. 2, pp. 273–292, 2016.
[38] M. Househ, R. Grainger, C. Petersen, P. Bamidis, and M. Merolli, "Balancing between privacy and patient needs for health information in the age of participatory health and social media: A scoping review," *Yearbook Med. Informat.*, vol. 27, no. 1, pp. 29–36, Aug. 2018.
[39] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset)," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, 2008.
[40] S. R. Stoyanov, L. Hides, D. J. Kavanagh, O. Zelenko, D. Tjondronegoro, and M. Mani, "Mobile app rating scale: A new tool for assessing the quality of health mobile apps," *JMIR mHealth uHealth*, vol. 3, no. 1, p. e27, Mar. 2015.
[41] A. Baumel, K. Faber, N. Mathur, J. M. Kane, and F. Muench, "Enlight: A comprehensive quality and therapeutic potential evaluation tool for mobile and Web-based eHealth interventions," *J. Med. Internet Res.*, vol. 19, no. 3, p. e82, Mar. 2017.
[42] R. Clarke, "Privacy impact assessment: Its origins and development," *Comput. Law Secur. Rev.*, vol. 25, no. 2, pp. 123–135, Jan. 2009.
[43] D. Wright, "The state of the art in privacy impact assessment," *Comput. Law Secur. Rev.*, vol. 28, no. 1, pp. 54–61, Feb. 2012.
[44] R. Armstrong, B. J. Hall, J. Doyle, and E. Waters, "Scoping the scope'of a cochrane review," *J. Public Health*, vol. 33, no. 1, pp. 147–150, 2011.
[45] General Data Protection Regulation, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46," *Off. J. Eur. Union*, vol. 59, pp. 1–88, Apr. 2016.
[46] D. Kotz, S. Avancha, and A. Baxi, "A privacy framework for mobile health and home-care systems," in *Proc. 1st ACM Workshop Secur. Privacy Med. Home-Care Syst. (SPIMACS)*, 2009, pp. 1–12.
[47] A. Alkussayer and W. H. Allen, "A scenario-based framework for the security evaluation of software architecture," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, vol. 5, Jul. 2010, pp. 687–695.
[48] M. M. Yusof, A. Papazafeiropoulou, R. J. Paul, and L. K. Stergioulas, "Investigating evaluation frameworks for health information systems," *Int. J. Med. Informat.*, vol. 77, no. 6, pp. 377–385, Jun. 2008.
[49] N. Prat, I. Comyn-Wattiau, and J. Akoka, "A taxonomy of evaluation methods for information systems artifacts," *J. Manage. Inf. Syst.*, vol. 32, no. 3, pp. 229–267, Jul. 2015.
[50] A. J. Dix, J. Finlay, G. D. Abowd, and R. Beale, *Human-Computer Interaction*. London, U.K.: Pearson Education, 2003, p. 258.
[51] T. Mabo, B. Swar, and S. Aghili, "A vulnerability study of mHealth chronic disease management (CDM) applications (apps)," in *Proc. World Conf. Inf. Syst. Technol.* Cham, Switzerland: Springer, 2018, pp. 587–598.
[52] T. Brüggemann, J. Hansen, T. Dehling, and A. Sunyaev, "An information privacy risk index for mHealth apps," in *Annual Privacy Forum*. Cham, Switzerland: Springer, 2016, pp. 190–201.

[53] H.-Y. Huang and M. Bashir, "Android app permission and users' adoption: A case study of mental health application," in *Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust*. Cham, Switzerland: Springer, 2017, pp. 110–122.

[54] C. Braghin, S. Cimato, and A. D. Libera, "Are mHealth apps secure? A case study," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2018, pp. 335–340.

[55] K. Huckvale, J. Torous, and M. E. Larsen, "Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation," *JAMA Netw. Open*, vol. 2, no. 4, 2019, Art. no. e192542.

[56] J. M. Robillard, T. L. Feng, A. B. Sporn, J.-A. Lai, C. Lo, M. Ta, and R. Nadler, "Availability, readability, and content of privacy policies and terms of agreements of mental health apps," *Internet Intervent.*, vol. 17, Sep. 2019, Art. no. 100243.

[57] J. Müthing, T. Jäschke, and C. M. Friedrich, "Client-focused security assessment of mHealth apps and recommended practices to prevent or mitigate transport security issues," *JMIR mHealth uHealth*, vol. 5, no. 10, p. e147, Oct. 2017.

[58] L. Rosenfeld, J. Torous, and I. V. Vahia, "Data security and privacy in apps for dementia: An analysis of existing privacy policies," *Amer. J. Geriatric Psychiatry*, vol. 25, no. 8, pp. 873–877, Aug. 2017.

[59] C. Stach and B. Mitschang, "The secure data container: An approach to harmonize data sharing with information security," in *Proc. 17th IEEE Int. Conf. Mobile Data Manage. (MDM)*, vol. 1, Jun. 2016, pp. 292–297.

[60] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," *Internet Intervent.*, vol. 15, pp. 110–115, Mar. 2019.

[61] J. Müthing, R. Brüngel, and C. M. Friedrich, "Server-focused security assessment of mobile health apps for popular mobile platforms," *J. Med. Internet Res.*, vol. 21, no. 1, p. e9818, Jan. 2019.

[62] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: The alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, 2018.

[63] T. Mulder, "Health apps, their privacy policies and the GDPR," *Eur. J. Law Technol.*, vol. 10, no. 1, pp. 1–20, 2019.

[64] S. M. Habib, N. Alexopoulos, M. M. Islam, J. Heider, S. Marsh, and M. Muehlhaeuser, "Trust4App: Automating trustworthiness assessment of mobile applications," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 124–135.

[65] J. Muchagata and A. Ferreira, "Mobile apps for people with dementia: Are they compliant with the general data protection regulation (GDPR)?" in *Proc. 12th Int. Joint Conf. Biomed. Eng. Syst. Technol.*, Jan. 2019, pp. 68–77.

[66] N. Tailor, Y. He, and I. Wagner, "POSTER: Design ideas for privacy-aware user interfaces for mobile devices," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2016, pp. 219–220.

[67] B. Olabenjo and D. Makaroff, "Information leakage in wearable applications," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, 2019, pp. 211–224.

[68] K. Grindrod, J. Boersema, K. Waked, V. Smith, J. Yang, and C. Gebotys, "Locking it down: The privacy and security of mobile medication apps," *Can. Pharmacists J./Revue Pharmaciens Canada*, vol. 150, no. 1, pp. 60–66, Jan. 2017.

[69] P.-A. Fougerouse, M. Yasini, G. Marchand, and O. O. Aalami, "A cross-sectional study of prominent us mobile health applications: Evaluating the current landscape," in *Proc. AMIA Annu. Symp.*, vol. 2017. Bethesda, MD, USA: American Medical Informatics Association, 2017, p. 715.

[70] S. A. Marotta-Walters, K. Jain, J. DiNardo, P. Kaur, and S. Kaligounder, "A review of mobile applications for facilitating EMDR treatment of complex trauma and its comorbidities," *J. EMDR Pract. Res.*, vol. 12, no. 1, pp. 2–15, 2018.

[71] A. Huguet, S. Rao, P. J. McGrath, L. Wozney, M. Wheaton, J. Conrod, and S. Rozario, "A systematic review of cognitive behavioral therapy and behavioral activation apps for depression," *PLoS ONE*, vol. 11, no. 5, May 2016, Art. no. e0154248.

[72] J. Povey, P. P. J. R. Mills, K. M. Dingwall, A. Lowell, J. Singer, D. Rotumah, J. Bennett-Levy, and T. Nagel, "Acceptability of mental health apps for aboriginal and torres strait islander australians: A qualitative study," *J. Med. Internet Res.*, vol. 18, no. 3, p. e65, Mar. 2016.

[73] T. Alessa, M. S. Hawley, E. S. Hock, and L. de Witte, "Smartphone apps to support self-management of hypertension: Review and content analysis," *JMIR mHealth uHealth*, vol. 7, no. 5, May 2019, Art. no. e13645.

[74] J. S. Loy, E. E. Ali, and K. Y.-L. Yap, "Quality assessment of medical apps that target medication-related problems," *J. Managed Care Specialty Pharmacy*, vol. 22, no. 10, pp. 1124–1140, Oct. 2016.

[75] P. Bondaronek, G. Alkhaldi, A. Slee, F. L. Hamilton, and E. Murray, "Quality of publicly available physical activity apps: Review and content analysis," *JMIR mHealth uHealth*, vol. 6, no. 3, p. e53, Mar. 2018.

[76] J. Liang, X. He, Y. Jia, W. Zhu, and J. Lei, "Chinese mobile health APPs for hypertension management: A systematic evaluation of usefulness," *J. Healthcare Eng.*, vol. 2018, pp. 1–14, Mar. 2018.

[77] F. Bert, S. Passi, G. Scaioli, M. R. Gualano, and R. Siliquini, "There comes a baby! What should I do? Smartphones' pregnancy-related applications: A Web-based overview," *Health Informat. J.*, vol. 22, no. 3, pp. 608–617, Sep. 2016.

[78] J. Hsu, D. Liu, Y. M. Yu, H. T. Zhao, Z. R. Chen, J. Li, and W. Chen, "The top Chinese mobile health apps: A systematic investigation," *J. Med. Internet Res.*, vol. 18, no. 8, p. e222, Aug. 2016.

[79] M. Maringer, P. van't Veer, N. Klepacz, M. C. D. Verain, A. Normann, S. Ekman, L. Timotijevic, M. M. Raats, and A. Geelen, "User-documented food consumption data from publicly available apps: An analysis of opportunities and challenges for nutrition research," *Nutrition J.*, vol. 17, no. 1, p. 59, Dec. 2018.

[80] K. S. Thach, "User's perception on mental health applications: A qualitative analysis of user reviews," in *Proc. 5th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Nov. 2018, pp. 47–52.

[81] M. Bachiri, A. Idri, J. L. Fernández-Alemán, and A. Toval, "Mobile personal health records for pregnancy monitoring functionalities: Analysis and potential," *Comput. Methods Programs Biomed.*, vol. 134, pp. 121–135, Oct. 2016.

[82] M. Yasini, J. Beranger, P. Desmarais, L. Perez, and G. Marchand, "mHealth quality: A process to seal the qualified mobile health apps," in *Exploring Complexity in Health: An Interdisciplinary Systems Approach*, A. Hoerbst *et al.*, Eds. Amsterdam, The Netherlands: IOS Press, 2016, doi: 10.3233/978-1-61499-678-1-205.

[83] K. Singh, K. Drouin, L. P. Newmark, J. Lee, A. Faxvaag, R. Rozenblum, E. A. Pabo, A. Landman, E. Klinger, and D. W. Bates, "Many mobile health apps target high-need, high-cost populations, but gaps remain," *Health Affairs*, vol. 35, no. 12, pp. 2310–2318, Dec. 2016.

[84] J. Zelmer, K. van Hoof, M. Notarianni, T. van Mierlo, M. Schellenberg, and C. Tannenbaum, "An assessment framework for e-Mental health apps in canada: Results of a modified delphi process," *JMIR mHealth uHealth*, vol. 6, no. 7, Jul. 2018, Art. no. e10016.

[85] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, and A. S. Albahri, "Conceptual framework for the security of mobile health applications on Android platform," *Telematics Informat.*, vol. 35, no. 5, pp. 1335–1354, Aug. 2018.

[86] R. N. Jeminiwa, N. S. Hohmann, and B. I. Fox, "Developing a theoretical framework for evaluating the quality of mHealth apps for adolescent users: A systematic review," *J. Pediatric Pharmacol. Therapeutics*, vol. 24, no. 4, pp. 254–269, Jul. 2019.

[87] C. Nebeker, R. J. B. Ellis, and J. Torous, "Development of a decision-making checklist tool to support technology selection in digital health research," *Transl. Behav. Med.*, p. ibz074, May 2019, doi: 10.1093/tbm/ibz074.

[88] S. Leigh, J. Ouyang, and C. Mimnagh, "Effective? Engaging? Secure? Applying the ORCHA-24 framework to evaluate apps for chronic insomnia disorder," *Evidence Based Mental Health*, vol. 20, no. 4, p. e20, Nov. 2017.

[89] J. C. Wyatt, "How can clinicians, specialty societies and others evaluate and improve the quality of apps for patient use?" *BMC Med.*, vol. 16, no. 1, p. 225, Dec. 2018.

[90] L. H. Iwaya, S. Fischer-Hübner, R.-M. Åhlfeldt, and L. A. Martucci, "Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats," *JMIR mHealth uHealth*, vol. 7, no. 3, Mar. 2019, Art. no. e11642.

[91] A. Mense, P. Urbauer, S. Sauermann, and H. Wahl, "Simulation environment for testing security and privacy of mobile health apps," in *Proc. Modeling Simulation Med. Symp.* Vista, CA, USA: Society for Computer Simulation International, 2016, Art. no. 2.

[92] K. Atchariyachanvanich, N. Mitinunwong, B. Tamthong, and N. Sonehara, "Determinants of personal health information disclosure: A case of mobile application," *Int. J. Softw. Innov.*, vol. 6, no. 1, pp. 31–43, Jan. 2018.

[93] K. Ghazinour, E. Shirima, V. R. Parne, and A. BhoomReddy, "A model to protect sharing sensitive information in smart watches," *Procedia Comput. Sci.*, vol. 113, pp. 105–112, Jan. 2017.

[94] F. Beierle, V. T. Tran, M. Allemand, P. Neff, W. Schlee, T. Probst, R. Pryss, and J. Zimmermann, "Context data categories and privacy model for mobile data collection apps," *Procedia Comput. Sci.*, vol. 134, pp. 18–25, Jan. 2018.
[95] E. Greene, P. Proctor, and D. Kotz, "Secure sharing of mHealth data streams through cryptographically-enforced access control," *Smart Health*, vol. 12, pp. 49–65, Apr. 2019.
[96] L. S. Vervier, A. C. Valdez, and M. Ziefle, "'Attitude'-mHealth apps and users' insights: An empirical approach to understand the antecedents of attitudes towards mHealth applications," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Ageing Well e-Health (ICTAWE)*, 2019, pp. 213–221.
[97] G. M. Turner-McGrievy, S. B. Hales, D. E. Schoffman, H. Valafar, K. Brazendale, R. G. Weaver, M. W. Beets, M. D. Wirth, N. Shivappa, T. Mandes, J. R. Hébert, S. Wilcox, A. Hester, and M. J. McGrievy, "Choosing between responsive-design websites versus mobile apps for your mobile behavioral intervention: Presenting four case studies," *Transl. Behav. Med.*, vol. 7, no. 2, pp. 224–232, Jun. 2017.
[98] J. B. McClure, J. Heffner, S. Hohl, P. Klasnja, and S. L. Catz, "Design considerations for mHealth programs targeting smokers not yet ready to quit: Results of a sequential mixed-methods study," *JMIR mHealth uHealth*, vol. 5, no. 3, p. e31, Mar. 2017.
[99] B. Marent, F. Henwood, M. Darking, and E. Consortium, "Development of an mHealth platform for HIV care: Gathering user perspectives through co-design workshops and interviews," *JMIR mHealth uHealth*, vol. 6, no. 10, p. e184, Oct. 2018.
[100] N. Jones and M. Moffitt, "Ethical guidelines for mobile app development within health and mental health fields," *Prof. Psychol., Res. Pract.*, vol. 47, no. 2, p. 155, 2016.
[101] F. Naeem, N. Gire, S. Xiang, M. Yang, Y. Syed, F. Shokraneh, C. Adams, and S. Farooq, "Reporting and understanding the safety and adverse effect profile of mobile apps for psychosocial interventions: An update," *World J. Psychiatry*, vol. 6, no. 2, p. 187, 2016.
[102] D. Ng, J. Mcmurray, J. Wallace, and P. Morita, "What is being used and who is using it: Barriers to the adoption of smartphone patient experience surveys," *JMIR Formative Res.*, vol. 3, no. 1, p. e9922, Mar. 2019.
[103] M. Dworkin, A. Chakraborty, S. Lee, C. Monahan, L. Hightow-Weidman, R. Garofalo, D. Qato, and A. Jimenez, "A realistic talking human embodied agent mobile phone intervention to promote HIV medication adherence and retention in care in young HIV-positive african American men who have sex with men: Qualitative study," *JMIR mHealth uHealth*, vol. 6, no. 7, Jul. 2018, Art. no. e10211.
[104] E. M. de Korte, N. Wiezer, J. H. Janssen, P. Vink, and W. Kraaij, "Evaluating an mHealth app for health and well-being at work: Mixed-method qualitative study," *JMIR mHealth uHealth*, vol. 6, no. 3, p. e72, Mar. 2018.
[105] R. Lipson-Smith, F. White, A. White, L. Serong, G. Cooper, G. Price-Bell, and A. Hyatt, "Co-design of a consultation audio-recording mobile app for people with cancer: The SecondEars app," *JMIR Formative Res.*, vol. 3, no. 1, Mar. 2019, Art. no. e11111.
[106] B. Roy, M. Call, and N. Abts, "Development of usability guidelines for mobile health applications," in *Proc. Int. Conf. Hum.-Comput. Interact.* Cham, Switzerland: Springer, 2019, pp. 500–506.
[107] M. N. Lind, M. L. Byrne, G. Wicks, A. M. Smidt, and N. B. Allen, "The effortless assessment of risk states (EARS) tool: An interpersonal approach to mobile sensing," *JMIR Mental Health*, vol. 5, no. 3, Aug. 2018, Art. no. e10334.
[108] M. Lang, M. Mayr, S. Ringbauer, and L. Cepek, "PatientConcept app: Key characteristics, implementation, and its potential benefit," *Neurol. Therapy*, vol. 8, no. 1, pp. 147–154, Jun. 2019.
[109] R. Alturki and V. Gay, "The development of an arabic weight-loss app akser waznk: Qualitative results," *JMIR Formative Res.*, vol. 3, no. 1, Mar. 2019, Art. no. e11785.
[110] K. Kretzschmar, H. Tyroll, G. Pavarini, A. Manzini, I. Singh, and NeurOx Young People's Advisory Group, "Can your phone be your therapist? Young people's ethical perspectives on the use of fully automated conversational agents (chatbots) in mental health support," *Biomed. Informat. Insights*, vol. 11, pp. 1–9, Feb. 2019.
[111] L. Zhou, J. Bao, V. Watzlaf, and B. Parmanto, "Barriers to and facilitators of the use of mobile health apps from a security perspective: Mixed-methods study," *JMIR mHealth uHealth*, vol. 7, no. 4, Apr. 2019, Art. no. e11223.
[112] J. Muchagata and A. Ferreira, "Translating GDPR into the mHealth practice," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2018, pp. 1–5.
[113] L. Zhou, B. Parmanto, Z. Alfikri, and J. Bao, "A mobile app for assisting users to make informed selections in security settings for protecting personal health data: Development and feasibility study," *JMIR mHealth uHealth*, vol. 6, no. 12, Dec. 2018, Art. no. e11210.
[114] A. Schreiber and R. Struminski, "Tracing personal data using comics," in *Proc. Int. Conf. Universal Access Hum.-Comput. Interact.* Cham, Switzerland: Springer, 2017, pp. 444–455.
[115] D. Nesheva, "Introduction to health information technologies," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 618, no. 1, 2019, Art. no. 012033.
[116] T. Ermakova, H. Krasnova, and B. Fabian, "Exploring the impact of readability of privacy policies on users' trust," in *Proc. Eur. Conf. Inf. Syst. (ECIS)*. İstanbul, Turkey: Boğaziçi Univ., Jun. 2016. [Online]. Available: https://aisel.aisnet.org/ecis2016_rp/20
[117] K. A. Bamberger, S. Egelman, C. Han, A. Elazari, and I. Reyes, "Can you pay for privacy? consumer expectations and the behavior of free and paid apps," *Berkeley Technol. Law J.*, vol. 35, Oct. 2020.
[118] W. Chipidza, D. Leidner, and D. Burleson, "Why companies change privacy policies: A principal-agent perspective," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 4849–4858.
[119] K. M. Beck, M. Beedle, A. V. Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, S. J. Mellor, K. Schwaber, J. Sutherland, and D. Thomas, "Manifesto for agile software development," Tech. Rep., 2013.
[120] P. Rozin and E. B. Royzman, "Negativity bias, negativity dominance, and contagion," *Personality Social Psychol. Rev.*, vol. 5, no. 4, pp. 296–320, Nov. 2001.
[121] P. F. Wu, "In search of negativity bias: An empirical study of perceived helpfulness of online reviews," *Psychol. Marketing*, vol. 30, no. 11, pp. 971–984, Nov. 2013.
[122] A. Mukherjee, V. Venkataraman, B. Liu, and N. Glance, "Fake review detection: Classification and analysis of real and pseudo reviews," Univ. Illinois Chicago, Chicago, IL, USA, Tech. Rep. UIC-CS-2013Ű03, 2013.
[123] M. Hertzum, "Images of usability," *Int. J. Hum.-Comput. Interact.*, vol. 26, no. 6, pp. 567–600, May 2010.

LEYSAN NURGALIEVA received the Ph.D. degree in information and communication technologies from the University of Trento, in June 2019. Since July 2019, she has been an ALECS Marie Skłodowska-Curie Postdoctoral Researcher with the Trinity College Dublin, Ireland. Her research interests include human–computer interaction, e-health, as well as user experience and privacy and security of digital health interventions.

DAVID O'CALLAGHAN received the Ph.D. degree in computer science from the Trinity College Dublin, in 2007. He is currently the Chief Information Security Officer at SilverCloud Health. His current research interests include data protection and security in digital health technology.

GAVIN DOHERTY received the D.Phil. degree in computer science from the University of York, in 1999. He is currently an Associate Professor and a Fellow with the Trinity College Dublin. His research interest includes human–computer interaction with a focus on the design of healthcare technologies and mental health technologies in particular. He is a Distinguished Member of ACM.