Published online: 2020-08-21





# Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019

Hannah K. Galvin[1, 2], Paul R. DeMuro[3]
[1] Cambridge Health Alliance, Cambridge, MA, USA
[2] Tufts University School of Medicine, Boston, MA, USA
[3] Chief Legal Officer Health and Wellness, Royal Palm Companies, Miami, Florida

## Summary

**Objectives**: To survey international regulatory frameworks that serve to protect privacy of personal data as a human right as well as to review the literature regarding privacy protections and data ownership in mobile health (mHealth) technologies between January 1, 2016 and June 1, 2019 in order to identify common themes.

**Methods**: We performed a review of relevant literature available in English published between January 1, 2016 and June 1, 2019 from databases including PubMed, Google Scholar, and Web of Science, as well as relevant legislative background material. Articles out of scope (as detailed below) were eliminated. We categorized the remaining pool of articles and discrete themes were identified, specifically: concerns around data transmission and storage, including data ownership and the ability to re-identify previously de-identified data; issues with user consent (including the availability of appropriate privacy policies) and access control; and the changing culture and variable global attitudes toward privacy of health data.

**Results**: Recent literature demonstrates that the security of mHealth data storage and transmission remains of wide concern, and aggregated data that were previously considered "de-identified" have now been demonstrated to be re-identifiable. Consumer-informed consent may be lacking with regard to mHealth applications due to the absence of a privacy policy and/or to text that is too complex and lengthy for most users to comprehend. The literature surveyed emphasizes improved access control strategies. This survey also illustrates a wide variety of global user perceptions regarding health data privacy.

**Conclusion**: The international regulatory framework that serves to protect privacy of personal data as a human right is diverse. Given the challenges legislators face to keep up with rapidly advancing technology, we introduce the concept of a "healthcare fiduciary" to serve the best interest of data subjects in the current environment.

## Keywords

Privacy, confidentiality, telemedicine, Health Insurance Portability and Accountability Act, international law

Yearb Med Inform 2020:32-43
http://dx.doi.org/10.1055/s-0040-1701987

## Introduction

Privacy has long been considered a human right [1-3]. Defined as the amount of personal data and information that people allow others to access about themselves [4], privacy in healthcare can be particularly important to patients [5] and may be threatened when technologies are employed to monitor the health and wellbeing of people [1]. Confidentiality is the process of keeping one's data private [4]. This is critical to medical practice as some people may not seek care or share sensitive information with a provider if they do not believe their data will be kept confidential [5, 6]. A breach of confidentiality, whether it be through data security vulnerabilities or otherwise, is a threat to one's privacy [1]; users will have less trust that their information is to be kept private, safe, and secure if it can easily be accessed and used by others. Data security relies on the technical, physical, and administrative safeguards that protect personal information held by an entity [7, 8].

Privacy, confidentiality, and data security are therefore very important concepts in healthcare today, while continual advances in technologies make it increasingly difficult to protect these concepts. In this article, we focus on mobile health (mHealth) technologies as one of these emerging areas that challenge the industry to revise and solidify its perspective in this regard. We chose mHealth given its rising ubiquity throughout the health care ecosystem as well as the fact that its porous nature poses key ethical and informatics challenges.

## Background: Global Privacy Laws

Information privacy has long been important in International Law [9]. The Fourth Amendment to the US Constitution is central to the US privacy law [10]. The Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, is central to European privacy law [11]. Although a seminal article in 1890 discussed the right to privacy [12], modern day privacy concepts evolved in part from Article 8 of The European Convention on Human Rights [13, 14] and a 1973 report by the future US Department of Health and Human Services (HHS), which encouraged Congress to adopt a "Code of Fair Information Practices" [15], and which led to the Privacy Act of 1974 [16]. These Fair Information Practices Principles (FIPP) have since served as a framework for the governance of personal data and spurred substantial growth in privacy law around the world [9, 17].

Europe: Informed by The European Convention on Human Rights, the General Data Protection Regulation (GDPR) was enacted in 2016, which automatically applies to all 27 member states in the European Union (EU) [18, 19]. Increasingly considered the gold standard for legal expertise in the area of health information privacy [20, 21], the GDPR has larger reach compared with previous models; in it, all individuals, organizations, and companies (not just those related to healthcare) are classified as either "controllers" (which determine the purposes and means of the processing of personal data) or "processors" (which perform operations on the data on behalf

of the controller) [22]. It also defines "personal data" much more broadly [22], as "any information relating to an identified or identifiable natural person" [18]. The GDPR provides a number of fundamental rights to data subjects, including those defined in Table 1 [18, 22]. Violations of the law may result in hefty fines, fines which depend on the severity of the infraction but can peak at 20 million euros or 4% of an entity's annual revenue worldwide [18]. Despite many criticisms, the GDPR has become the current gold standard, given its attention to personal data privacy and data portability. In the context of health care data, such focus is a particularly valuable asset [23].

United States: In 1996, the United States passed the Health Insurance Portability and Accountability Act (HIPAA), which was the first US federal statute to address the privacy of medical records, and considered the well-known model for regulation in this area until promulgation of the GDPR [8, 9, 24]. FIPP and HIPAA both recognize that individuals should be able to (1) access their individually identifiable health information, (2) correct its accuracy and integrity, and (3) trust that their information will be collected, used, and disclosed consistent with their expectations through openness and transparency. In addition, an individual should be able to make informed consent about such information, which should only be collected, used, and disclosed to the extent necessary for a particular purpose. Data quality and integrity should be maintained through security safeguards and organizational accountability [17]. HIPAA is a compliance-oriented regulatory model which does not provide for a private right of action [25]. The HITECH Act of 2009 subsequently enhanced penalties for HIPAA violations, expanded enforcement, and added a data breach notification requirement [9, 26]. HIPAA has a number of limitations, including the fact that it does not cover all medical records (only those maintained by certain types of record holders) and that it does not cover all parties that possess medical information [9, 27, 28]. It is therefore important to note that HIPAA does not cover many websites that gather health information [9]. Privacy laws in the United States additionally do not provide for comprehensive regulation and do not account for technological innovation [29]. Instead, various government agencies hold specified responsibilities. The U.S. HHS Office for Civil Rights plays the main role in enforcing HIPAA. The Food and Drug Administration regulates the efficacy and safety of medical devices [30] and has proposed voluntary cybersecurity guidance for connected medical devices [27-29, 31, 32]. The Federal Trade Commission may regulate unfair and deceptive trade practices in or affecting commerce, which may include deceptive acts which fail to adhere to state privacy policies and procedures [27, 29, 33]. That said, certain particularly sensitive health information has been addressed by subsequent federal legislation such as the Genetic Information Nondiscrimination Act of 2008 (GINA), which seeks to prohibit discrimina-

**Table 1** Selected data subject rights provided in GDPR [18, 22]

| Article | Data Subject Right | Definition |
|---|---|---|
| 13 | Right to be informed | Data subjects have the right to be provided with certain information from a data controller that has collected their data. |
| 15 | Right to access information | Data subjects have the right to obtain confirmation from a data controller as to whether or not their personal data are being processed and, if so, to access that data and certain information. |
| 16 | Right to rectification | Data subjects have the right to correct inaccurate personal data held by a controller and to complete personal data that is incomplete. |
| 17 | Right to erasure | Also known as "the right to be forgotten," data subjects have the right to request that the controller of their personal data erase certain data concerning them which has been made public, taking account of available technology and the cost of implementation. The controller shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data of the request. |
| 18 | Right to restriction of processing | Data subjects have the right to set restrictions on the processing of their data by a controller in certain instances. |
| 20 | Right to data portability | Data subjects have the right to receive their personal data from a controller in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without any hindrance from the controller providing the data. |
| 21 | Right to object to the processing of personal data | Data subjects have the right to object at any time, on situation-specific grounds, to the processing of personal data concerning them. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or the processing is necessary for the performance of a task carried out for reasons of public interest. |
| 22 | Right to object to automated decision-making | Data subjects have the right not to be subject to any individual decision based solely on automated processing, including profiling, if such a decision leads to significant ramifications (legal and otherwise), subject to certain exceptions. |

tion on the basis of genetic information with respect to health insurance and employment. This includes information about genetic tests, services or research obtained, or manifestation of a genetic disease by an individual or their family members [34].

At the state level, California passed the California Consumer Privacy Act of 2018 (CCPA), heavily influenced by the GDPR, with an effective date of January 1, 2020 [35, 36]. Given the limitations of US federal law noted above, the CCPA is the most comprehensive set of data privacy laws and individual protections in the United States to date [19]. The CCPA takes an even more expansive approach than the GDPR with respect to its definition of "personal information," as being any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" [37, 38]. While the GDPR regulates data processing, the CCPA also regulates collection and sale of data, but does not provide a safe harbor for GDPR compliance [38, 39]. A subsequent California Senate Bill amended the CCPA in a number of ways, including clarifying that certain identifiers are no longer automatically included within the definition of "personal information" and that a consumer's right to litigation only applies to data breaches [36]. Although the fines for violation of the CCPA are less severe than the GDPR [35], both pieces of legislation have resulted in changes in the behaviors of large multinational corporations [40], and, given the broader definitions applied and the rights incurred to citizens, are rapidly becoming the de facto global standards for data privacy and protection [20, 21].

South America: On August 14, 2018, Brazil enacted its first legislation that provides for the data protection of individuals and private and public legal entities, which will go into effect with modifications in 2020 [41, 42]. This General Data Protection Law was largely inspired by the GDPR [43] and defines personal data to include "data related to the health or sexual life of a person, genetic information, or biometric data." [42]. The Argentina Personal Data Protection Act or Protection of Personal Information Act (POPIA) has been in effect since 2000 [44]. However, the Argentinian government has recently proposed a bill to bring this law in line with the GDPR, including new definitions such as biometric and genetic data [45].

Asia: In 2005, the Asia-Pacific Economic Cooperation (APEC) established the APEC Privacy Framework [46], which was updated in 2015 [47]. To implement this Framework, APEC developed the Cross-Border Privacy Rules System Program Requirements [48]. APEC economies endorsed the Privacy Framework because it is important in the development of appropriate information privacy protections to ensure the flow of information in the region [46]. It is consistent with the core values of The Organization for Economic Cooperation and Development's (OECD's) Guidelines on the Protection of Privacy and Trans-Boundary Flows of Personal Data. The OECD, a global organization of countries committed to the market economy and personal democracy which had created guidelines for the protection of privacy information in 1980 [49, 50], adopted a revised Recommendation Concerning Guidelines Governing the Principles of Transborder Flows of Personal Data in 2013 [51]. This was non-binding and in and around that time period, many countries around the world adopted data protection laws based on its Information Privacy Principles. The APEC Cross Border Privacy Rules system (CBPR) has broad areas of similarity with the current GDPR, but whereas the GDPR is based on the individual's fundamental right to data protection and privacy within a union in which data is freely-flowing, the APEC CBPR focuses on facilitating data transfers across borders within the context of its defined data protection parameters [52].

Japan has had one of the earliest privacy laws in Asia, the Act on the Protection of Personal Information (APPI), enacted in 2003 [53]. It was extensively amended and significantly enhanced in May 2017, one year before the GDPR [53, 54]. The APPI now defines "sensitive personal data to include physical or mental disabilities, results of certain medical exams, records of medical treatment and advice" [42].

When it was enacted in 2011, South Korea's Personal Information Protection Act (PIPA) was Asia's toughest data privacy law [55, 56, 42]. PIPA defines "sensitive personal data" to include health, sexual preferences, and bio-data" [42]. The country additionally has a sector-specific law, known as the "Network Act," which governs information and communication service providers [57].

On November 6, 2016, China passed the Cybersecurity Law of the People's Republic of China, which was effective the following June [58]. While this legislation does not regulate all aspects of privacy and cybersecurity, it does have a wide scope and includes many broadly defined terms making it open to interpretation [59]. From a security standpoint, the law focuses on the protection of infrastructure and data storage requirements. From a privacy perspective, it pulls from other countries' legislation regarding informed consent and the use of personal information for a limited purpose. Like the GDPR, it adds an individual right to question correctness or request deletion of personal information [60, 61].

Africa: South Africa signed the Protection of Personal Information Act (POIPA) into law on November 19, 2013 [62, 63]. Under POIPA, "special personal information" includes data on an individual's health, sex life, or biometric information, but unlike the GDPR, data subjects can waive their right to a privacy notice [62]. Further regulations were promulgated under POIPA in 2018 [64].

In February 2019, Uganda enacted the Data Protection and Privacy Act (DPPA), which provides rights for and protects the privacy of citizens by regulating the obligations of data collectors, processors, and controllers. As such, it prohibits these entities from collecting, holding, and processing personal data which infringes on the privacy of a data subject [65].

In November of the same year, Kenya signed into law the Data Protection Act (DPA), which was preceded by the Privacy and Data Protection Act of 2018. This new law, modeled after the GDPR, outlines the rights of individuals whose data is collected and regulates the collection and processing of data by a data controller or processor. It also provides for certain protections for processing of sensitive personal data and personal data relating to health [66].

Australia: Australia Privacy Principles (APPs) form the basis for the privacy protection in the Privacy Act 1988, which was amended in 2018 to add mandatory notification procedure for data breaches, which must

take into consideration the sensitivity of the information [64, 67-71]. Additional privacy regulations include applicable state and territory laws, which may relate specifically to health privacy [72]. If an organization participates in the Australian eHealth system, it must comply with the Personally Controlled Electronic Records Act of 2012 (PCEHR Act) [73] and the Health Identifiers Act of 2010 (HI Act) [69-71]. In the context of these laws, "sensitive information" includes heath, genetic, and biometric information [72]. The PCEHR limits when and how health information in an electronic health record can be collected, used, and disclosed.

## Methods

We performed a review of relevant literature available in English published between January 1, 2016 and June 1, 2019 from databases including PubMed, Google Scholar, and Web of Science. Search terms included: "data ownership," "data sharing," "privacy," "data privacy," "genetic privacy," "confidentiality," "data security," "computer security," "Health Insurance Portability and Accountability Act," "protecting data," or "data protection" combined with any of the following: "mobile health," "mhealth," "health app," "direct-to-consumer genetic testing," "direct-to-consumer genetic screening," or "telemedicine," as well as relevant abbreviations and lexical variants of the above. Search strings are available as Supplemental File 1.

Articles focused solely on techncal specifications or security protocols, research-based initiatives, and traditional telemedicine (i.e., through videoconferencing) were determined to be out of scope. In addition, given the abundance of literature meeting criteria, the authors decided to further limit the scope by eliminating articles related solely to consumer genetic testing. We categorized the remaining pool of ar-

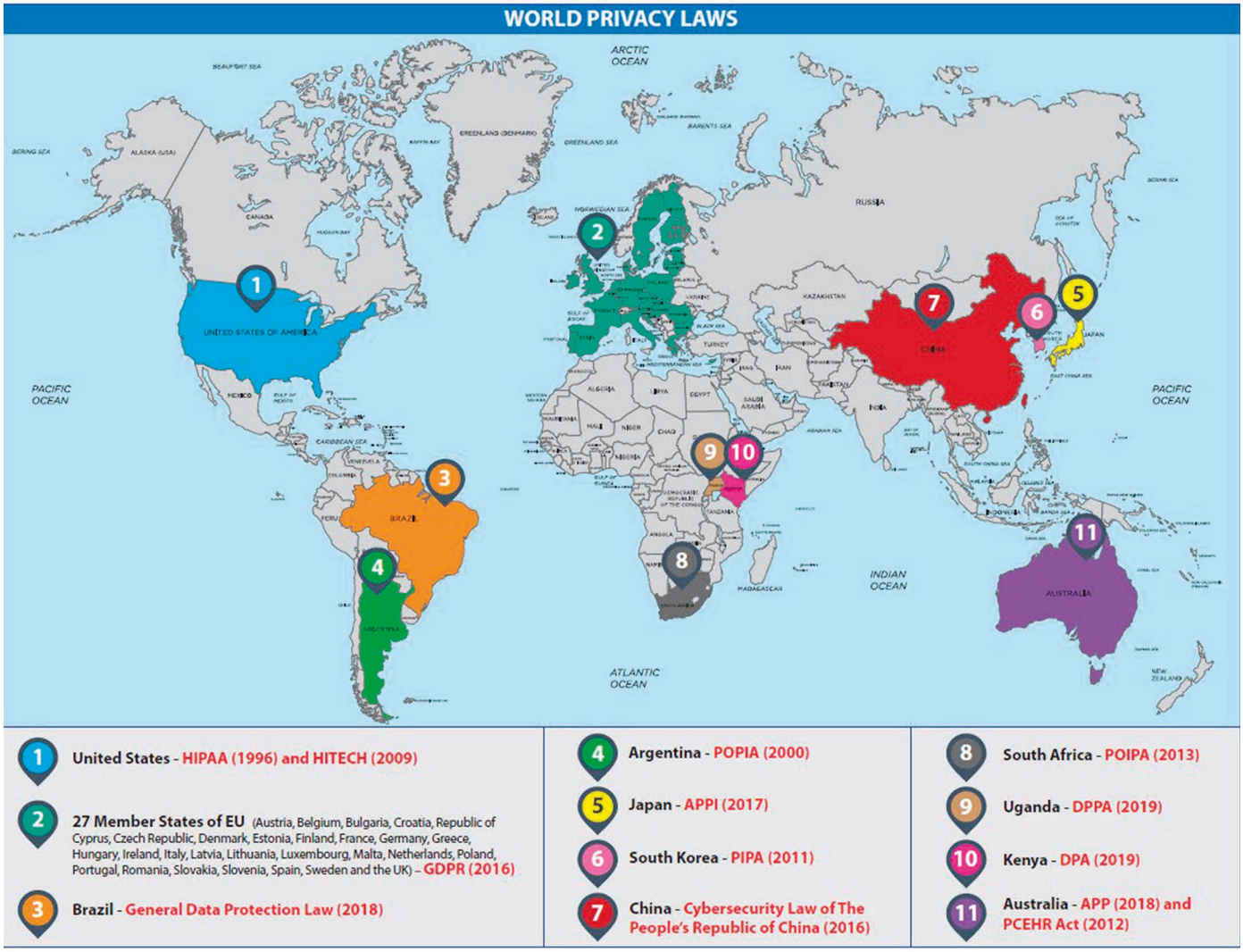


**Fig. 1** World Privacy Laws

ticles as pertaining to (1) Issues regarding mHealth privacy and security, (2) User perceptions and attitudes related to such, or (3) Related ethical, legal, governance, or policy frameworks. From the first two categories, we identified a number of discrete themes, specifically: concerns around data transmission and storage, including data ownership and the ability to re-identify previously de-identified data; issues with user consent (including the availability of appropriate privacy policies) and access control; and the changing zeitgeist and variable global attitudes toward privacy of health data. These themes are addressed in detail below and serve, along with material from the final category, to inform the authors' discussion and conclusions.

# Themes

## Data Transmission and Storage

Mobile app data security continues to be an area of concern for the industry. Many authors discuss the vulnerabilities of data when being stored or during transmission to third parties [28, 74, 75]. There is still some debate in the literature about the security risks and benefits of the cloud; while some authors fear that cloud infrastructure is more susceptible to privacy and security attacks [76], others postulate that cloud service providers may address data privacy and security more effectively due to economies of scale and scope, which enable them to maintain more sophisticated defenses against cyber-attacks [77].

Physical security is also an issue. Authors express concerns about misplacement, theft, or loss of mobile devices [78, 79]. More than 1/3 of smartphone users do not apply security measures to prevent access to their phone, and sharing of phones among family members is common in many countries [80, 81].

It is certainly evident that many mHealth apps on the market lack appropriate privacy and security measures. This has been found to be the case even among many apps certified by trusted bodies or widely used by the health care community. For example, of 79 apps certified as being clinically safe and trustworthy by the United Kingdom National Health Service, 89% were found to transfer information online, 66% of which was not encrypted [82-85]. WhatsApp, a popular instant messaging app that has gained popularity among clinical providers and in the global health space as being supposedly HIPAA-compliant did not have security measures such as end-to-end encryption for some time; now, even with additional security measures in place, concerns still exist around whether these are sufficient to meet HIPAA security standards [86-88]. In a study of 20 of the most popular "Medical" and "Health and Fitness" apps, only 20% of those that transmitted data over the network did so using a secure connection [89]. In another study of 137 selected mHealth apps, more than 60% allowed for transmission of health information via insecure methods [90]. Similarly, in a study of 53 mHealth apps available in the EU, 21% failed to protect session data in transport [91].

That same study showed that 40% of the apps failed to protect the integrity of the data they displayed [91]. Other authors also expressed concerns that data integrity could be compromised as a result of attacks during transmission over public networks or simply due to immature sensor-based technology [74, 75, 78, 80, 92]. Another oft-cited concern regarding data collected outside of the clinical setting regards its authenticity, accuracy, and provenance [92, 93]. Securely tagging such data with metadata could help in attributing authenticity of authorship. Additionally, methods for collecting and presenting contextual information, such as whether a blood pressure cuff was applied correctly, need to be developed. As such, mHealth apps are creating new silos of data which can be a challenge to integrate into electronic health record and health information exchange ecosystems [94].

Numerous stakeholders (including patients, providers, healthcare systems, government bodies, technical service vendors, and network infrastructure suppliers) hold intersecting rights and responsibilities regarding an individual medical record and the data therein. "Ownership" of such data involves questions of who possesses or allows access to it and who gains from any intellectual property that may subsequently be developed [74, 95]. Commercial institutions or vendors may sell de-identified information to data brokers who may then indefinitely own a patient's data and use it for a variety of purposes, including targeted ads or larger profiling efforts [27]. This type of aggregate data mining by third parties can still be linked back to the individual. In 2000, Latanya Sweeney first demonstrated that 87% of the US population (216 million people) could be uniquely identified from only their data of birth, gender, and 5-digit zip code [96-98]. More recently, she demonstrated the ability to correctly identify 25% of research participants by name and 28% by address from data redacted beyond the HIPAA Safe Harbor standard [99]. Other authors have demonstrated the ability to re-identify at least 90% of Americans utilizing credit card metadata or via statistical models [96, 100, 101]. Given this emerging area of research, the need to systemically identify all stakeholders and potential data "owners" becomes increasingly essential in the identification of potential downstream security risks to users.

## Informed Consent, Privacy Policies, and Access Control

Informed consent, in the context of mHealth applications, involves the permission granted by patients or their legal representative regarding when and with whom their personal information is shared [74]. This, along with mechanisms to enable individual control of data, supports the ethical frameworks of autonomy or respect for persons, as well as beneficence and non-maleficence [95, 102, 103].

Consumers are often unaware of all of the ways a service may collect and analyze their data or the extent to which their data may be sent to third parties [104]. Transparency, therefore, is of the utmost importance. However, the literature is consistent in its illustration of the mHealth industry as being poorly compliant with the provision of appropriate privacy policies or Terms of Service agreements to users [84, 89, 90, 105-113]. Where privacy policies do exist, they are often non-specific to the app in question, may not inform users if the policy is being updated or if their data is to be shared, and

may not provide users the right to access their personal data or be otherwise HIPAA-non-compliant [107, 108, 110, 114-116].

Although Article 12 of the GDPR requires that companies explain how data will be processed in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" [18], most mHealth app privacy policies studied have been found to be roughly the length of an academic journal article and have a readability at university level [107, 113, 117], making them inaccessible to a large percentage of consumers and posing a risk for inequity between the highly-educated who are able to comprehend their privacy rights and options and the rest of the population. Users often agree on the assumption of minimal risk, as reading dense policies is onerous and time-consuming [118-120]. Moreover, while Article 7 of the GDPR specifies that information sharing as a condition of use may prohibit consent from being "freely given" if processing of data is not necessary for performance of such a contract [18], the literature notes that users are frequently required to agree to data sharing in order to access relevant mHealth devices and services [79, 121], which may also predispose them to agree to privacy policies or terms without full perusal or understanding.

Multiple authors, therefore, recommend increasing education to improve digital literacy and citizenship, both among professionals and patients [74, 122, 123]. Some authors additionally point out the "notice and choice paradigm" whereby the limited user interfaces inherent to many mHealth products make it difficult to surface adequate notice of privacy policies; while vendors can and do send their policy statements through e-mail, the user may not directly associate them with the app or wearable [33]. Therefore, several propose "just in time" strategies for requesting user consent and other modalities to improve policy effectiveness [107, 124]. That said, one author notes that even among educated users who were aware that consenting to a company's terms of use constituted a legal contract, very few reported reading the agreements before consenting to them [125].

It has also been noted that, when creating such policies, application developers are truly challenged to fully anticipate and identify all third-party stakeholders and potential data streams for inclusion. For instance, many of the commonly-used software development kits (SDKs) for mobile apps rely on companies that do not explicitly state how user information is shared; moreover, in at least one case, an SDK was found to be accessing user data from its product apps via private APIs [126, 127]. To assist with such challenges, the United States Office of the National Coordinator for Health IT (ONC) has designed a Model Privacy Notice, "a voluntary, openly available resource that can provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users" [128].

Although privacy policies are of critical importance, research suggests that users are often set at ease regarding their privacy, and data sharing is more likely to occur when procedures are put in place that provide individuals with control over disclosure and subsequent use of their personal information [129]. User trust can be established by allowing clear understanding, choice, and control; therefore, multiple authors recommend providing users with as much control over their data as possible, including granular control over sharing of that data with third parties [79, 97, 130]. In the context of mobile apps, control over an application's access to other device functionality is of utmost importance. In a recent study of mHealth apps, a number of them were found to request "dangerous" permissions to access areas that involve the user's private information or stored data, including those outside of the applications' scope, such as the use of the microphone, Bluetooth connectivity, the user's contacts or calendar [89]. When wearables or ambient living systems are involved, issues of surveillance, including location disclosure and capturing bystanders without their consent are of great concern and require appropriate access control [124, 130-132].

## Dynamic User Attitudes Toward Privacy

Our survey also highlighted changes in user attitudes and variability across cultures regarding privacy of personal health data. Individual privacy protection expectations in open data sharing environments are both relative (depending on which parties may receive said data) and time-dependent, in that risk of sharing may either diminish or increase over time [133]. The concept of privacy could therefore be considered a moving target.

We have summarized user perceptions of privacy in Supplemental Table 1. From this literature, we make the following observations:

1. User concern with privacy of personal data collected by mobile health apps is widely variable. In some studies, data privacy and security was cited as of primary concern or importance [74, 134, 138], while in others, users expressed very little concern [125, 139-145]. Still other authors noted this dichotomy within their reported results with some participants expressing significant privacy concerns and others stating it to not be an issue [146, 147]. While some users expressed such concerns related to collection of highly sensitive-data, such as that related to behavioral health, reproductive health, or HIV status [135, 148-151], other users who provided such data still reported little unease related to their privacy [139, 142, 152-154].
2. Recent mHealth interventions in developing countries have frequently involved text message reminders. While fewer overall privacy and security concerns were generally reported by users in these countries, sharing of phones was stated to be a significant area for consideration [139-141, 149, 151, 153, 155, 156].
3. In some settings, professionals and caregivers expressed greater concern than the patients they served regarding the security of personal health data [155, 157, 158].
4. Higher expressed privacy, confidentiality and/or security concerns were often negatively correlated with technology acceptance and use [145, 151, 157, 159-162].
5. There may be international variation and/or gradual cultural shifts in user awareness regarding the risks inherent in big data. While participants in an American study reported that viewing of their personal health data was innocuous since it was likely only valuable in aggregate [125], a larger study in the UK (where the GDPR is now in effect) reported concerns about transfer of their data both

under their real identity as well as under a random pseudonym [114], suggesting an understanding of the risks of re-identification of pseudonymized data.

## Discussion

This survey of recent developments related to privacy, confidentiality, and data security of mHealth applications demonstrates that the global information technology industry and health care ecosystem which it supports remain in a dynamic and rapidly-maturing state. Although many countries and federations have enacted legislation to define and protect the right to privacy of personal data for individuals, there remain concerns that regulatory supervision is inadequate. As methods of data transfer become increasingly complex, the risk for compromise of highly sensitive patient health data also increases [31, 163]. Currently, much information is being processed without the knowledge and informed consent of the people who generated the data [164]. Even where measures such as the GDPR attempt to provide protections, gaps in local law may pose a challenge for technology design. For instance, though Spain and Czechoslovakia are members of the EU, Spanish law defines where and under which measures data should be physically stored, whereas Czech law does not [165]. It is thus not currently feasible to adopt international privacy standards that would cover all the health care data that currently exists and to anticipate new data streams that may emerge from developing technologies. mHealth apps are also increasingly being used in developing countries, which may have no privacy or data protection laws [79]. Additional legal provisions are therefore arising to support such gaps, such as the recent Planet 49 decision, in which the Court of Justice of the European Union ruled, in line with the GDPR, that privacy consent must be given by a clear affirmative act as opposed to pre-ticked boxes [166].

Risks related to data storage and transmission, as well as the re-identification of aggregated data, are real but may not be universally recognized by the general public [125]. User perceptions of privacy and concerns related to confidentiality of personal data are widely variable (see Supplemental Table 1). Even individuals concerned with protecting their confidentiality may not choose to fully inform themselves regarding the risks of disclosure and sharing of that data through the use of a mobile health app or service, often due to the impenetrable language and lengthy format of such privacy policies. Users do, however, commonly request increased choice and control over their data, and app developers grapple with how to enable such granular controls and display them according to usability heuristics. Additionally, consumers seem to be starting to recognize that pseudonymized data shared in aggregate may not be as private as previously thought [114], which poses further challenges to vendors and data brokers to consider privacy protections related to big data.

Our current global environment, therefore, is one in which local and international legislation continues its attempts to keep up with rapidly-advancing technological developments, but one in which significant gaps in policy and regulatory frameworks are inevitable. In such a dynamic state, some have argued that any entity in possession of an individual's data (that is, the "holder" of that data, which controls it and could seek to profit from it to the detriment of the individual) stands in a position of trust with regard to that person. One expert suggests "that many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries through their customers and end-users." [167].

A fiduciary has a legal obligation to act in the best interest of its client [170]. Therefore, we and others have suggested that entities which hold personal health data (such as mHealth app vendors, data brokers, and third parties with whom they share data) be therefore considered "health care information fiduciaries." [169, 170]. Further definition of this concept based on the type of health care information possessed, how such information was generated, the intended recipients and purpose of transmittal, as well as potential benefits a holder might derive from the data could help to further clarify this proposed role and the obligations that could ensue. If the concept of a health care fiduciary was recognized in a democracy, that concept should be upheld and interpreted by the applicable courts. If the concept was recognized in a dictatorship, it could likely be subject to the interpretation of that dictator. Additional analysis of how such a role would be regulated is a subject for future exploration [169, 170].

## Conclusion

In summary, the international regulatory framework that serves to protect privacy of personal data as a human right is diverse and increasingly influenced by the GDPR. This framework serves as a new model to define data as relating to the person (instead of the transaction) and to provide additional rights to the individual such as the right to object to processing and the right to erasure. As the law is evolving, the literature regarding mHealth applications over the past several years demonstrates that the security of data storage and transmission remains a concern, and the question of data "ownership" is complicated by the multiple stakeholders who have access to such data in the current ecosystem, often without the knowledge of the subject of the data. Consumers are often uneducated regarding the ways a service may collect and transmit their data to third parties; yet even when they are aware of the implication of vendor terms of service, most users do not read these policies before consenting due to policy length and complexity. While there is a wide variation in user perspectives of privacy – even those related to traditionally sensitive data types – there is evidence that improved access control measures are beneficial to the acceptance of technology and data sharing. Challenges arise in consideration of data aggregation, previously considered to be de-identified, as this has now been demonstrated to commonly be re-identifiable through a variety of mechanisms. Given that legislation is unable to keep up with the rapidly-advancing technology and consumer education and self-advocacy is limited, the concept of a "health care fiduciary" will be a fertile area for discussion as a means to act in the best interests of data subjects, and in so doing, to protect the basic human right of privacy in an equitable fashion across a dynamic ecosystem.

## References


1. Alkhatib S, Waycott J, Buchanan G, Bosua R. Privacy and the Internet of Things (IoT) Monitoring Solutions of Older Adults: A Review. Comput Inf Syst Univ Melb 2016.
2. Council of Europe. European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. European Court of Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf. Published 2010.
3. United Nations. Universal Declaration of Human Rights. https://www.un.org/en/universal-declaration-human-rights/. Published 1948.
4. Keller SA, Shipp S, Schroeder A. Does Big Data Change the Privacy Landscape? A Review of the Issues. Annu Rev Stat Its Appl 2016;3(1):161-80.
5. Zevon E, Patlak M, Nass S. Improving Cancer Diagnosis and Care: Clinical Application of Computational Methods in Precision Oncology: Proceedings of a Workshop. In: The National Academies Press; 2019. https://doi/org/10.17226/s5404.
6. Kaplan B. How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales. Cambridge Q Healthc Ethics 2016;25(2):312-29.
7. McGeveran W. The Duty of Data Security. Minn Law Rev 2019;103:1135.
8. Health Insurance Portability and Accountability Act of 1996.; 1996:Pub. L. No. 104-191, 110 Stat. 1936.
9. Mathews K. Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age. In: Practising Law Institute. 2nd ed. Proskauer; 2016.
10. US Constitution Amendment IV.
11. European Court of Human Rights. The Convention for the Protection of Human Rights and Fundamental Freedoms. Council of Europe; 1998:ETS No. 155.
12. Warren S, Brandeis L. The Right to Privacy. Harv L Rev 1890;4(5):193-220.
13. European Court of Human Rights. Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life. Council of Europe. https://www.refworld.org/docid/5a016ebe5.html. Published 2019.
14. Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols Nos. 11 and 14.; 1950. https://www.refworld.org/docid/3ae6b3b04.html.
15. U.S. Department of Health Education & Welfare. Records, Computers and the Rights of Citizens; 1973. https://www.justice.gov/opcl/docs/reccom-rights.pdf.
16. U.S. Privacy Act of 1974.; 1974:Pub L. No. 93-579, 88 Stat. 1896 (2000) (codified. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.
17. Baker DB, Kaye J, Terry SF. Privacy, Fairness, and Respect for Individuals. EGEMS (WashDC) 2016;4(2).
18. European Parliament and of the Council. Regulation (EU) 2016/679 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/EC (General Data Protection Regulation). Off J Eur Communities. 2016;OJ L 119/1:1-88. http://data.europa.eu/eli/reg/2016/679/oj.
19. Barrett C. Are the EU GDPR and the California CCPA becoming the de factor global standards for data privacy and protection? TheSciTechLawyer 2019.
20. Buttarelli G. The EU GDPR as a clarion call for a new global digital gold standard. LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_fr. Published 2016.
21. Kpadonou M. With the GDPR, Europe Shows the World the Way. Leaders League. https://www.leadersleague.com/en/news/with-the-gdpr-europe-shows-the-world-the-way. Published 2019.
22. Glassner U. Blockchain in EU E-Health – Blocked by the Barrier of Data Protection? Compliance Elliance J 2018;4(1).
23. Heinemann S. Data Power to the Patients! Patient-Driver Data Business, Not Data-Driven Patient Business. Compliance Elliance J 2018;4(2).
24. Yang C, Lin H, Chang P, Jian W. Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA. Comput Methods Programs Biomed 2006;82:277-282.
25. Terry NP, Wiley LF. Liability for Mobile Health and Wearable Technologies. Vol 47; 2014.
26. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA); 2009:Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009).
27. Armontrout J, Torous J, Fisher M, Drogin E, Gutheil T. Mobile Mental Health: Navigating New Rules and Regulations for Digital Tools. Curr Psychiatry Rep 2016;18(10).
28. Prochaska JJ, Coughlin SS, Lyons EJ. Social Media and Mobile Technology for Cancer Prevention and Treatment. Am Soc Clin Oncol Educ book Am Soc Clin Oncol Annu Meet 2017;37:128-137.
29. Nahara K, Corbin B. Digital Health Regulatory Gaps in the United States. Compliance Elliance J 2018;4(2).
30. U.S. Food and Drug Administration. Medical Device Overview. https://www.fda.gov/industry/regulated-products/medical-device-overview. Published 2018.
31. Kuhn A, Heinz M-I. Digitization in the Health Sector in the Trade-Off Between Technical and Legislative Possibilities and Legal Limits According to German Law. Compliance Elliance J 2018;4(2).
32. Kao CK, Liebovitz DM. Consumer Mobile Health Apps: Current State, Barriers, and Future Directions. PM R 2017;9(5S):S106-S115.
33. Shahmiri BS. Wearing Your Data on Your Sleeve : Wearables , the FTC , and the Privacy Implications of this New Technology. Texas Rev Entertain Sport Law 2016;18(1):25-49.
34. Congress US. H.R. 493 (110th): Genetic Information Nondiscrimination Act of 2008; 2008:L. 110-233, 122 Stat.881. https://www.govtrack.us/congress/bills/110/hr493/summary.
35. California Consumer Privacy Act of 2018.; 2018:Cal. Civ. Code, §§1798.100 – 1798.199.
36. Senate Bill No. 1121, Chapter 735. California State Senate; 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.
37. Jerome J. California Privacy Law Shows Data Protection is on the March. Am Bar Assoc Antitrust 2018;33(1).
38. California Consumer Privacy Act of 2018 Part 4. Obligations Arising from Particular Transactions.; 2018:Cal. Civ. Code §1798.140(o)(1).
39. Hirsch W, ML K, Hadgis K, Groebe L. The Proposed CCPA Regulations are Here: An Overview. Morgan Lewis. https://www.morganlewis.com/pubs/the-proposed-ccpa-regulations-are-here-an-overview. Published 2019.
40. Gallagher B. Why Multinational Companies Need to Care About GDPR Compliance. IS Partners LLC. https://www.ispartnersllc.com/blog/multinational-companies-gdpr-compliance. Published 2018.
41. Congress TN. Law No. 13,709, of August 14, 2018 – Provides for the Protection of Personal Data and Changes Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law"); 2018.
42. "What is the principal data protection legislation?". In: Relevant Legislation and Competent Authorities. BRAZIL, Chapter 9. http://www.iclg.com.
43. Brazil Adopts General Data Protection Law. Natl Law Rev 2019.
44. Congress TS and TH of R of the AN in. ACT 25,326, Personal Data Protection Act, Chapter 1, General Provisions; 2000.
45. Buerger S. How the GDPR changed the Argentina Personal Data Protection Act. Michalsons Pract Leg Solut 2017.
46. APEC Secretariat. APEC Privacy Framework. www.apec.org. Published 2005.
47. APEC Secretariat. APEC Privacy Framework (2015). www.apec.org. Published 2017.
48. Asia-Pacific Economic Cooperation. APEC Cross-Border Privacy Rules System Program Requirements. https://cbprs.blob.core.windows.net/files/Cross Border Privacy Rules Program Requirements.pdf.
49. Rotenberg M. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In: Privacy Law Sourcebook; 2002.
50. Reidenberg JR. Restoring Americans' Privacy in Electronic Commerce. Berkeley Technol Law J 1999;14:771.
51. Organisation for Economic Co-Operation and Development (. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013); 2013. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
52. Sullivan C. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. Comput Law Secur Rev 2019;35(4):380-97.
53. Beyond the GDPR: What You Should Know about Japan's Act on the Protection of Personal

Information. Focal Point Insights 2018.
54. Personal Information Protection Commission J. Amended Act on the Protection of Personal Information, Version 2; 2016.
55. Hayashi H. What is the principal data protection legislation? In: Relevant Legislation and Competent Authorities. JAPAN. Chapter 25.
56. Greenleaf G, Park W-I. Korea's new Act: Asia's toughest data privacy law. Priv Laws Bus Int Rep 2012;(117):1-6.
57. Personal Information Protection Act.; 2011: Chapter 1 General Provisions.
58. Creemers R, Triolo P, Webster G. Translation: Cybersecurity Law of the People's Republic of China. DigiChina 2017.
59. Bowman C, Li Y, Hou L. A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization. Proskauer 2017.
60. Lable C, Sussman H, Xiao M, Chen D. An In-Depth Examination of China's New Cybersecurity Law. Part I: Who Must Comply? Ropes Gray Alert, Priv Data Secur 2017.
61. Balke L. China's New Cybersecurity Law and U.S-China Cybersecurity Issues. Santa Clara Law Rev 2018;48(1).
62. Act on Promotion of Information and Communication Network Utilization and Information Protection; Chapter 1 General Provisions.
63. The Protection of Personal Information Act (POPIA); 2013:Act No. 4 of 2013.
64. Protection of Personal Information Act, 2013. Gov Gazette, Repub South Africa 2013;58(37067).
65. The Republic of Uganda. The Data Protection and Privacy Act, 2019; 2019:ACT Supplements No. 9, Vol. CXXI No. 21.
66. Kenya Gazette Supplement. The Data Protection Act; 2019: No. 181, §24.
67. Development SAD of J and C. Protection of Personal Information Act, 2013 (Act. No. 4 of 2013); Regulations Relating to the Protection of Personal Information; 2018: No R. 1383.
68. Innes K. The Privacy Act is Changing on 22 February 2018 – This is not a drill! AUSTRAILIA 2018.
69. Office of Parliamentary Counsel CA. Healthcare Identifiers Act of 2010; 2017: No. 72, 2010. Compilation No. 14 date July 1, 2017.
70. Office of Parliamentary Counsel CA. Privacy Act 1988, Compilation No. 77; 2018: No. 119, 1988. Compilation No. 77 date February 22.
71. Legislation AGFR of. Personally Controlled Electronic Health Records Act 2012: An Act to Provide for a System of Access to Electronic Health Records, and for Related Purposes; 2012: No. 63, 2012.
72. Office of Parliamentary Counsel CA. Privacy Act 1988, Compilation No. 81; 2019:No. 119. Compilation No. 81 date: August 13, 2019.
73. Privacy Guide: A guide to compliance with privacy laws in Australia. In: Justice Connect Not-for-Profit Law. Australia Not-for-Profit Law Guide; 2017.
74. Segura Anaya LH, Alsadoon A, Costadopoulos N, Prasad PWC. Ethical Implications of User Perceptions of Wearable Devices. Sci Eng Ethics 2018;24(1):1-28.
75. Bhuyan SS, Kim H, Isehunwa OO, Kumar N, Bhatt J, Wyant DK, et al. Privacy and security issues in mobile health: Current research and future directions. Health Policy Technol 2017;6(2):188-91.
76. Spanakis EG, Santana S, Tsiknakis M, Marias K, Sakkalis V, Teixeira A, et al. Technology-based innovations to foster personalized healthy lifestyles and well-being:a targeted review. J Med Internet Res 2016;18(6).
77. Roski J, Bo-Linn GW, Andrews TA. Creating value in health care through big data: Opportunities and policy implications. Health Aff 2014;33(7):1115-22.
78. Els F, Cilliers L. Improving the information security of personal electronic health records to protect a patient's health information. 2017 Conf Inf Commun Technol Soc ICTAS 2017 - Proc 2017;(March 2017).
79. Katusiime J, Pinkwart N. A review of privacy and usability issues in mobile health systems: Role of external factors. Health Informatics J October 2017:1460458217733121.
80. Wood PW, Boulanger P, Padwal RS. Home Blood Pressure Telemonitoring: Rationale for Use, Required Elements, and Barriers to Implementation in Canada. Can J Cardiol 2017;33(5):619-25.
81. Ippoliti NB, L'Engle K. Meet us on the phone: mobile phone programs for adolescent sexual and reproductive health in low-to-middle income countries. Reprod Health 2017;14(1):11.
82. Iglesias-Posadilla D, Gomez-Marcos V, Hernandez-Tejedor A. Apps and intensive care medicine. Med intensiva 2017;41(4):227-36.
83. Torous J, Nicholas J, Larsen ME, Firth J, Christensen H. Clinical review of user engagement with mental health smartphone apps: evidence, theory and improvements. Evid Based Ment Health 2018;21(3):116-9.
84. Treskes RW, van der Velde ET, Barendse R, Bruining N. Mobile health in cardiology: a review of currently available medical apps and equipment for remote monitoring. Expert Rev Med Devices 2016;13(9):823-30.
85. Huckvale K, Prieto JT, Tilney M, Benghozi PJ, Car J. Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. BMC Med 2015;13(1):1-13.
86. Calleja-Castillo JM, Gonzalez-Calderon G. WhatsApp in stroke systems: Current use and regulatory concerns. Front Neurol 2018;9(MAY):1-5.
87. Mars M, Escott R. WhatsApp in clinical practice: A literature review. Stud Health Technol Inform 2016;231:82-90.
88. Tazegul G, Bozoglan H, Ogut TS, Balci MK. A clinician's artificial organ? Instant messaging applications in medical care. Int J Artif Organs 2017;40(9):477-80.
89. Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. IEEE Access 2018;6:9390-403.
90. Singh K, Drouin K, Newmark LP, Lee JH, Faxwaag A, Rozenblum R, et al. Many Mobile Health Apps Target High-Need, High-Cost Populations, But Gaps Remain. Health Aff (Millwood) 2016;35(12):2310-8.
91. Müthing J, Jäschke T, Friedrich CM. Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues. JMIR MHealth UHealth 2017;5(10):e147.
92. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and Security in Mobile Health: A Research Agenda. Computer (Long Beach Calif) 2016;49(6):22-30.
93. Tofighi B, Abrantes A, Stein MD. The Role of Technology-Based Interventions for Substance Use Disorders in Primary Care: A Review of the Literature. Med Clin North Am 2018;102(4):715-31.
94. Mamlin BW, Tierney WM. The Promise of Information and Communication Technology in Healthcare: Extracting Value from the Chaos. Am J Med Sci 2016;351(1):59-68.
95. Balthazar P, Harri P, Prater A, Safdar NM. Protecting Your Patients' Interests in the Era of Big Data, Artificial Intelligence, and Predictive Analytics. J Am Coll Radiol 2018;15(3):580-6.
96. Davis J, Osoba O. Privacy Preservation in the Age of Big Data: A Survey. Priv Preserv Age Big Data A Surv. 2016:1-15.
97. Mohr DC, Zhang M, Schueller SM. Personal Sensing: Understanding Mental Health Using Ubiquitous Sensors and Machine Learning. Annu Rev Clin Psychol. 2017;13:23-47.
98. Sweeney L. Simple demographics often identify people uniquely. Carnegie Mellon Univ Data Priv Work Pap 3 Pittsburgh 2000:1-34. http://dataprivacylab.org/projects/identifiability/paper1.pdf.
99. Sweeney L, Yoo JS, Perovich L, Boronow KE, Brown P, Brody JG. Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study. Technol Sci 2017.
100. de Montjoye Y-A, Radaelli L, Singh VK, Pentland AS. Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 2015;347(6221):536-9.
101. Rocher L, Hendrickx JM, de Montjoye Y-A. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 2019;10(1):3069.
102. Bakken S, Marden S, Arteaga SS, et al. Behavioral Interventions Using Consumer Information Technology as Tools to Advance Health Equity. Am J Public Health 2019;109(S1):S79-S85.
103. Chung J, Demiris G, Thompson HJ. Ethical Considerations Regarding the Use of Smart Home Technologies for Older Adults: An Integrative Review. Annu Rev Nurs Res 2016;34:155-81.
104. Mense A, Steger S, Sulek M, Jukicsunaric D, Mészáros A. Analyzing privacy risks of mhealth applications. Stud Health Technol Inform 2016;221:41-5.
105. Parker L, Karliychuk T, Gillies D, Mintzes B, Raven M, Grundy Q. A health app developer's guide to law and policy: a multi-sector policy analysis. BMC Med Inform Decis Mak 2017;17(1):141
106. Rosenfeld L, Torous J, Vahia I V. Data Security and Privacy in Apps for Dementia : An Analysis of Existing Privacy Policies. Am J Geriatr Psychiatry 2019;25(8):873-7.
107. Sunyaev A, Dehling T, Taylor PL, Mandl KD.

Availability and quality of mobile health app privacy policies. J Am Med Informatics Assoc 2015;22(e1):e28-e33.
108. Minen MT, Stieglitz EJ, Sciortino R, Torous J. Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. Headache 2018;58(7):1014-27.
109. Bert F, Passi S, Scaioli G, Gualano MR, Siliquini R. There comes a baby! What should i do? Smartphones' pregnancy-related applications: A web-based overview. Health Informatics J 2016;22(3):608-17.
110. Blenner SR, Kollmer M, Rouse AJ, Daneshvar N, Williams C, Andrews LB. Privacy policies of android diabetes apps and sharing of health information: In reply. JAMA 2016;315(10):1053-4.
111. Huckvale K, Torous J, Larsen ME. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. JAMA Netw open 2019;2(4):e192542.
112. O'Loughlin K, Neary M, Adkins EC, Schueller SM. Reviewing the data security and privacy policies of mobile apps for depression. Internet Interv 2019;15:110-5.
113. Robillard JM, Feng TL, Sporn AB, Lai J-A, Lo C, Ta M, et al. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. Internet Interv 2019;17:100243.
114. Leibenger D, Möllers F, Petrlic A, Petrlic R, Sorge C. Privacy Challenges in the Quantified Self Movement – An EU Perspective. Proc Priv Enhancing Technol 2016;2016(4):315-34.
115. Bachiri M, Idri A, Fernandez-Aleman JL, Toval A. Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring. J Med Syst 2018;42(8):144.
116. Hutton L, Price BA, Kelly R, McCormick C, Bandara AK, Hatzakis T, et al. Assessing the Privacy of mHealth Apps for Self-Tracking: Heuristic Evaluation Approach. JMIR MHealth UHealth 2018;6(10):e185.
117. Powell AC, Singh P, Torous J. The Complexity of Mental Health App Privacy Policies: A Potential Barrier to Privacy. JMIR MHealth UHealth 2018;6(7):e158.
118. Bruggemann T, Hansen J, Dehling T, Sunyaev A. An Information Privacy Risk Index for mHealth Apps 2016;8319(September).
119. Glenn T, Monteith S. Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections. Curr Psychiatry Rep 2014;16(11).
120. Martinez-Martin N, Kreitmair K. Ethical Issues for Direct-to-Consumer Digital Psychotherapy Apps: Addressing Accountability, Data Protection, and Consent. JMIR Ment Health 2018;5(2):e32.
121. Schairer CE, Rubanovich CK, Bloss CS. How could commercial terms of use and privacy policies undermine informed consent in the age of mobile health? AMA J Ethics 2018;20(9):E864-E872.
122. Fernandez-Luque L, Staccini P. All that Glitters Is not Gold: Consumer Health Informatics and Education in the Era of Social Media and Health Apps. Findings from the Yearbook 2016 Section on Consumer Health Informatics. Yearb Med Inform 2016;(1):188-93. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&CSC=Y&NEWS=N&PAGE=fulltext&D=med12&AN=27830250.
123. Edwards-Stewart A, Alexander C, Armstrong CM, Hoyt T, O'Donohue W. Mobile applications for client use: Ethical and legal considerations. Psychol Serv 2019;16(2):281-5.
124. Parker L, Halter V, Karliychuk T, Grundy Q. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. Int J Law Psychiatry 2019;64:198-204.
125. Ostherr K, Borodina S, Bracken RC, Lotterman C, Storer E, Williams B. Trust and privacy in the context of user-generated health data. Big Data Soc 2017;4(1):205395171770467.
126. Owen JE, Kuhn E, Jaworski BK, McGee-Vincent P, Juhasz K, Hoffman JE, et al. VA mobile apps for PTSD and related problems: public health resources for veterans and those who care for them. mHealth 2018;4:28.
127. Perez S. Hundreds Of Apps Banned From App Store For Accessing Users' Personal Information. TechCruch 2015. https://techcrunch.com/2015/10/19/hundreds-of-apps-banned-from-app-store-for-accessing-users-personal-information/.
128. Office of the National Coordinator of Health Information Technology. 2016 Model Privacy Notice. https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf. Published 2016.
129. Moore D, Niemi M. The Sharing of Personal Health Data – A Review of the Literature; 2016;(June).
130. Perez AJ, Zeadally S. Privacy Issues and Solutions for Consumer Wearables. IT Prof 2018;20(4):46-56.
131. Liddle J, Burdon M, Ireland D, Carter A, Knuepffer C, Milevskiy N, et al. Balancing Self-Tracking and Surveillance: Legal, Ethical and Technological Issues in Using Smartphones to Monitor Communication in People with Health Conditions. J Law Med 2016;24(2):387-97. http://www.ncbi.nlm.nih.gov/pubmed/30137711.
132. Mortenson W Ben, Sixsmith A, Beringer R. No Place Like Home? Surveillance and What Home Means in Old Age. Can J Aging 2016;35(1):103-14.
133. Sánchez D, Viejo A. Personalized privacy in open data sharing scenarios. Online Inf Rev 2017;41(3):298-310. http://10.0.4.84/OIR-01-2016-0011%0Ahttp://search.ebscohost.com/login.aspx?direct=true&db=llf&AN=123252056&site=ehost-live.
134. Haluza D, Naszay M, Stockinger A, Jungwirth D. Prevailing opinions on connected health in Austria: Results from an online survey. Int J Environ Res Public Health 2016;13(8).
135. Bucci S, Morris R, Berry K, Berry N, Haddock G, Barrowclough C, et al. Early Psychosis Service User Views on Digital Technology: Qualitative Analysis. JMIR Ment Health 2018;5(4):e10091.
136. McClure JB, Hartzler AL, Catz SL. Design Considerations for Smoking Cessation Apps: Feedback From Nicotine Dependence Treatment Providers and Smokers. JMIR MHealth UHealth 2016;4(1):e17.
137. Saberi P, Siedle-Khan R, Sheon N, Lightfoot M. The Use of Mobile Health Applications Among Youth and Young Adults Living with HIV: Focus Group Findings. AIDS Patient Care STDS 2016;30(6):254-60.
138. Torous J, Wisniewski H, Liu G, Keshavan M. Mental Health Mobile Phone App Usage, Concerns, and Benefits Among Psychiatric Outpatients: Comparative Survey Study. JMIR Ment Health 2018;5(4):e11715.
139. Biswas KK, Hossain A, Chowdhury R, Andersen K, Sultana S, Shahidullah SM, et al. Using mHealth to Support Postabortion Contraceptive Use: Results From a Feasibility Study in Urban Bangladesh. JMIR Form Res 2017;1(1):e4.
140. Eckersberger E, Pearson E, Andersen K, Hossain A, Footman K, Biswas KK, et al. Developing mHealth Messages to Promote Postmenstrual Regulation Contraceptive Use in Bangladesh: Participatory Interview Study. JMIR MHealth UHealth 2017;5(12):e174.
141. Hoque MR, Bao Y, Sorwar G. Investigating factors influencing the adoption of e-Health in developing countries: A patient's perspective. Informatics Health Soc Care 2017;42(1):1-17.
142. Brody C, Tatomir B, Sovannary T, Pal K, Mengsrun S, Dionosio J, et al. Mobile phone use among female entertainment workers in Cambodia: an observation study. mHealth 2017;3:3.
143. Feinberg L, Menon J, Smith R, Rajeev JG, Kumar RK, Banerjee A. Potential for mobile health (mHealth) prevention of cardiovascular diseases in Kerala: A population-based survey. Indian Heart J 2017;69(2):182-99.
144. Leenan LAM, Wijnen BFM, de Kinderen RJA, van Heugten CM, Evers SMAA, Majoie MHJM. Are people with epilepsy using eHealth-tools? Epilepsy Behav 2016;64:268-72.
145. van Kerkhof LWM, van der Laar CWE, de Jong C, Weda M, Hegger I. Characterization of Apps and Other e-Tools for Medication Use: Insights Into Possible Benefits and Risks. JMIR MHealth UHealth 2016;4(2):e34.
146. de Korte EM, Wiezer N, Janssen JH, Vink P, Kraaij W. Evaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study. JMIR MHealth UHealth 2018;6(3):e72.
147. Cheung C, Bietz MJ, Patrick K, Bloss CS. Privacy attitudes among early adopters of emerging health technologies. PLoS One 2016;11(11):1-12.
148. Zhao Y, Zhu X, Perez AE, Zhang W, Shi A, Zhang Z, et al. MHealth approach to promote Oral HIV self-testing among men who have sex with men in China: a qualitative description. BMC Public Health 2018;18(1):1146.
149. Ronen K, Unger JA, Drake AL, Perrier T, Akinyi P, Osborn L, et al. SMS messaging to improve ART adherence: perspectives of pregnant HIV-infected women in Kenya on HIV-related message content. AIDS Care 2018;30(4):500-5.
150. Stawarz K, Preist C, Tallon D, Wiles N, Coyle D. User Experience of Cognitive Behavioral Therapy Apps for Depression: An Analysis of App Functionality and User Reviews. J Med Internet Res 2018;20(6):e10120.

151. Campbell JI, Aturinda I, Mwesigwa E, Burns B, Santorino D, Haberer JE, et al. The Technology Acceptance Model for Resource-Limited Settings (TAM-RLS): A Novel Framework for Mobile Health Interventions Targeted to Low-Literacy End-Users in Resource-Limited Settings. AIDS Behav 2017;21(11):3129-40.
152. Marent B, Henwood F, Darking M. Development of an mHealth platform for HIV Care: Gathering User Perspectives Through Co-Design Workshops and Interviews. JMIR MHealth UHealth 2018;6(10):e184.
153. van der Kop M, Muhula S, Ekström AM, Jongbloed K, Smillie K, Abunah B, et al. Participation in a mobile health intervention trial to improve retention in HIV care: does gender matter? J Telemed Telecare 2017;23(2):39-46.
154. Bauer AM, Iles-Shih M, Ghomi RH, Rue T, Grover T, Kincler N, et al. Acceptability of mHealth augmentation of Collaborative Care: A mixed methods pilot study. Gen Hosp Psychiatry 2018;51:22-9.
155. Nhavoto JA, Gronlund A, Klein GO. Mobile health treatment support intervention for HIV and tuberculosis in Mozambique: Perspectives of patients and healthcare workers. PLoS One 2017;12(4):e0176051.
156. Moodley J, Constant D, Botha MH, van der Merwe FH, Edwards A, Momberg M. Exploring the feasibility of using mobile phones to improve the management of clients with cervical cancer precursor lesions. BMC Womens Health 2019;19(1):2.
157. Hendrikoff L, Kambeitz-Ilankovic L, Pryss R, Senner F, Falkai P, Pogarell O, et al. Prospective acceptance of distinct mobile mental health features in psychiatric patients and mental health professionals. J Psychiatr Res 2019;109:126-32.
158. Liu Y, Wang L, Chang P, Lamb K V, Cui Y, Wua Y. What features of smartphone medication applications are patients with chronic diseases and caregivers looking for? Stud Health Technol Inform 2016;225:515-9.
159. Puri A, Kim B, Nguyen O, Stolee P, Tung J, Lee J. User Acceptance of Wrist-Worn Activity Trackers Among Community-Dwelling Older Adults: Mixed Method Study. JMIR MHealth UHealth 2017;5(11):e173.
160. Deng Z, Hong Z, Ren C, Zhang W, Xiang F. What Predicts Patients' Adoption Intention Toward mHealth Services in China: Empirical Study. JMIR MHealth UHealth 2018;6(8):e172.
161. Rasche P, Wille M, Bröhl C, et al. Prevalence of health app use among older adults in Germany: National survey. J Med Internet Res 2018;20(1):1-11.
162. Abelson JS, Kaufman E, Symer M, Peters A, Charlson M, Yeo H. Barriers and benefits to using mobile health technology after operation: A qualitative study. Surgery 2017;162(3):605-11.
163. Montgomery F. Cf. speech of the president of the German Medical Association and the German Physicians' Board, Prof. Dr. Frank Ulrich Montgomery, Opening of the 121st German Physicians' Board in the Steigerwaldstadion Erfurt on the 8th of May 2018. https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/121.DAET/Eroeffnungsrede_Prof._Montgomery.pdf. Published 2018.
164. Mendelson D, Mendelson D. Legal protections for personal health information in the age of Big Data — a proposal for regulatory framework. Ethics, Med Public Heal 2017;3(1):37-55.
165. Lhotska L, Cheshire P, Pharow P, Macku D. Non-technical issues in design and development of personal portable devices. Stud Health Technol Inform 2016;221:46-50.
166. Barcelo R, Ciesielka A YE. The Planet49 Decision: Key Takeaways. LexBlog. https://www.lexblog.com/2019/10/01/the-planet49-decision-key-takeaways/. Published 2019.
167. Dobkin A. Information Fiduciaries in Practice: Data Privacy and User Expectations. Berkeley Technol Law J 2018;33(1):1.
168. Balkin JM. Information Fiduciaries and the First Amendment. UC Davis Law Rev 2016;49(4):1183.
169. DeMuro P, Petersen C. Managing Privacy and Data Sharing Through the Use of Health Care Information Fiduciaries. Stud Heal Technol Inform 2019;265:157-62.
170. DeMuro P, Galvin H. Patient-Generated Health Data and Healthcare Information Fiduciaries. In: Emerging Technologies in Healthcare - Legal, Ethical & Social Aspects. London, UK; 2019.
171. Nicholas J, Boydell K, Christensen H. Beyond symptom monitoring: Consumer needs for bipolar disorder self-management using smartphones. Eur Psychiatry 2017;44:210-6.
172. Nicholas J, Huckvale K, Larsen ME, Basu A, Batterham PJ, Shaw F, et al. Issues for eHealth in psychiatry: Results of an expert survey. J Med Internet Res 2017;19(2).
173. Nicholas J, Fogarty AS, Boydell K, Christensen H. The reviews are in: A qualitative content analysis of consumer perspectives on apps for bipolar disorder. J Med Internet Res 2017;19(4).
174. Muigg D, Kastner P, Modre-Osprian R, Haluza D, Duftschmid G. Is Austria ready for Telemonitoring? A readiness assessment among doctors and patients in the field of diabetes. Stud Health Technol Inform 2018;248:322-9.
175. Duftschmid G, Modre-Osprian R, Muigg D, Haluza D, Kastner P. Readiness to use telemonitoring in diabetes care: a cross-sectional study among Austrian practitioners. BMC Med Inform Decis Mak 2019;7:1-10.
176. Baskerville NB, Dash D, Wong K, Shuh A, Abramowicz A. Perceptions Toward a Smoking Cessation App Targeting LGBTQ+ Youth and Young Adults: A Qualitative Framework Analysis of Focus Groups. JMIR Public Heal Surveill 2016;2(2):e165.
177. Basterfield A, Dimitropoulos G, Bills D, Cullen O, Freeman VE. "I would love to have online support but I don't trust it": Positive and negative views of technology from the perspective of those with eating disorders in Canada. Health Soc Care Community 2018;26(4):604-12.
178. Woldeyohannes HO, Ngwenyama OK. Factors Influencing Acceptance and Continued Use of mHealth Apps. 2017;10293:239-56.
179. Li H, Wu J, Gao Y, Shi Y. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. Int J Med Inform 2016;88(555):8-17.
180. Goetz M, Müller M, Matthies LM, Hansen J, Doster A, Szabo A, et al. Perceptions of Patient Engagement Applications During Pregnancy: A Qualitative Assessment of the Patient's Perspective. JMIR MHealth UHealth 2017;5(5):e73.
181. Hartmann R, Sander C, Lorenz N, Böttger D, Hegerl U. Utilization of patient-generated data collected through mobile devices: Insights from a survey on attitudes toward mobile self-monitoring and self-management apps for depression. J Med Internet Res 2019;21(4):1-18.
182. Holderried M, Ernst C, Holderried F, Rieger M, Blumenstock G, Tropitzsch A. The potential of eHealth in otorhinolaryngology-head and neck surgery: patients' perspectives. Eur Arch Otorhinolaryngol 2017;274(7):2933-43.
183. Kessel KA, Vogel MM, Schmidt-Graf F, Combs SE. Mobile Apps in Oncology: A Survey on Health Care Professionals' Attitude Toward Telemedicine, mHealth, and Oncological Apps. J Med Internet Res 2016;18(11):e312.
184. Rasche P, Wille M, Bröhl C, Theis S, Schäfer K, Knobe M, et al. Prevalence of Health App Use Among Older Adults in Germany: National Survey. JMIR MHealth UHealth 2018;6(1):e26.
185. Griebel L, Kolominsky-Rabas P, Schaller S, Siudyka J, Sierpinski R, Papapavlou D, et al. Acceptance by laypersons and medical professionals of the personalized eHealth platform, eHealthMonitor. Inform Health Soc Care 2017;42(3):232-49.
186. Van Velsen L, Wildevuur S, Flierman I, Van Schooten B, Tabak M, Hermens H. Trust in telemedicine portals for rehabilitation care: An exploratory focus group study with patients and healthcare professionals eHealth/ telehealth/ mobile health systems. BMC Med Inform Decis Mak 2016;16(1):1-12.
187. Hossain I, Lim ZZ, Ng JJ Le, Koh WJ, Wong PS. Public attitudes towards mobile health in Singapore: a cross-sectional study. mHealth 2018;4:41.
188. Cilliers L. Wearable devices in healthcare: Privacy and information security issues. Health Inf Manag May 2019:1833358319851684.
189. Aicken CRH, Fuller SS, Sutcliffe LJ, Estcourt CS, Gkatzidou V, Oakeshott P, et al. Young people's perceptions of smartphone-enabled self-testing and online care for sexually transmitted infections: Qualitative interview study. BMC Public Health 2016;16(1):1-11.
190. Berry N, Lobban F, Bucci S. A qualitative exploration of service user views about using digital health interventions for self-management in severe mental health problems. BMC Psychiatry 2019;19(1):35.
191. Burrows A, Coyle D, Gooberman-Hill R. Privacy, boundaries and smart homes for health: An ethnographic study. Health Place 2018;50:112-8.
192. Greenfield R, Busink E, Wong CP, Riboli-Sasco E, Greenfield G, Majeed A, et al. Truck drivers' perceptions on wearable devices and health promotion: A qualitative study. BMC Public Health 2016;16(1):1-10.
193. Griffin N, Kehoe M. A questionnaire study to explore the views of people with multiple sclerosis of using smartphone technology for health care

purposes. Disabil Rehabil 2018;40(12):1434-42.
194. Perski O, Blandford A, Ubhi HK, West R, Michie S. Smokers' and drinkers' choice of smartphone applications and expectations of engagement: a think aloud and interview study. BMC Med Inform Decis Mak 2017;17(1):25.
195. Abelson JS, Kaufman E, Symer M, Peters A, Charlson M, Yeo H. Barriers and benefits to using mobile health technology after operation: A qualitative study. Surgery 2017;162(3):605-11.
196. Bauer AM, Rue T, Munson SA, Ghomi RH, Keppel GA, Cole AM, et al. Patient-oriented health technologies: Patients' perspectives and use. J Mob Technol Med 2017;6(2):1-10.
197. Bietz MJ, Bloss CS, Calvert S, Godino JG, Gregory J, Claffey MP, et al. Opportunities and challenges in the use of personal health data for health research. J Am Med Inform Assoc 2016;23(e1):1-7.
198. Garg SK, Lyles CR, Ackerman S, Handley MA, Schillinger D, Gourley G, et al. Qualitative analysis of programmatic initiatives to text patients with mobile devices in resource-limited health systems. BMC Med Inform Decis Mak 2016;16(1):1-12.
199. Lipschitz J, Miller CJ, Hogan TP, Burdick KE, Lippin-Foster R, Simon SR, et al. Adoption of Mobile Apps for Depression and Anxiety: Cross-Sectional Survey Study on Patient Interest and Barriers to Engagement. JMIR Ment Health 2019;6(1):e11334.
200. Lowens B, Motti VG, Caine K. Wearable Privacy: Skeletons in the Data Closet. Proc - 2017 IEEE Int Conf Healthc Informatics, ICHI 2017. 2017:295-304.
201. Nicholas J, Shilton K, Schueller SM, Gray EL, Kwasny MJ, Mohr DC. The Role of Data Type and Recipient in Individuals' Perspectives on Sharing Passively Collected Smartphone Data for Mental Health: Cross-Sectional Questionnaire Study. JMIR MHealth UHealth 2019;7(4):e12578.
202. Ofili EO, Pemu PE, Quarshie A. Democratizing Discovery Health with N = Me. Trans Am Clin Climatol Assoc 2018;(129):215-34.
203. Place S, Blanch-Hartigan D, Rubin C, Gorrostieta C, Mead C, Kane J, et al. Behavioral Indicators on a Mobile Sensing Platform Predict Clinically Validated Psychiatric Symptoms of Mood and Anxiety Disorders. J Med Internet Res 2017;19(3):e75.
204. Sedlander E, Barboza KC, Jensen A, Skusky N, Bennett K, Sherman S, et al. Veterans' Preferences for Remote Management of Chronic Conditions. Telemed J E Health 2018;24(3):229-35.
205. Serrano KJ, Yu M, Riley WT, Patel V, Hughes P, Marchesini K, et al. Willingness to exchange health information via mobile devices: Findings from a population-based survey. Ann Fam Med 2016;14(1):34-40.
206. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. JMIR MHealth UHealth 2019;7(4):e11223.

**Correspondence to:**
Hannah K. Galvin, MD, FAAP, ABPM-CI
Tufts University School of Medicine
145 Harrison Ave
Boston, MA 02111
USA
E-mail: hgalvinmd@gmail.com