# A Taxonomy of mHealth Apps – Security and Privacy Concerns

Miloslava Plachkinova
Claremont Graduate University
miloslava.plachkinova@cgu.edu

Steven Andrés
Claremont Graduate University
steven.andres@cgu.edu

Samir Chatterjee
Claremont Graduate University
samir.chatterjee@cgu.edu

## Abstract

*With the increasing use of smartphones for healthcare purposes, more and more people now share their personal healthcare information using a variety of applications. The vast number of existing mobile health (mHealth) applications creates a serious problem for users, as often times they are unaware of how their data are managed and used. We propose a taxonomy incorporating the most significant security and privacy aspects of mHealth applications. This artifact can help outline some of the problems related to creating and downloading mHealth applications. The taxonomy was tested with 38 top-rated Android and iOS healthcare applications. Results of the evaluation suggest that having a unified mechanism to categorize mHealth applications with respect to security and privacy is important and can be beneficial. This study contributes to literature, as it builds upon prior work and adds knowledge to a still new and relatively unexplored domain such as mobile healthcare.*

## 1. Introduction

Smartphones are increasingly viewed as handheld computers due to their improved computing capabilities [1]. The acceptance and adoption of these devices is growing due to their improved ease of use [2]. Smartphones are used by physicians to access patient records, to view test results, and to prescribe medications [3-5]. Patients also use smartphones to access and update their medical records, to monitor their health statistics, and to view their prescriptions [6]. The impact of mobile applications (apps) on reducing healthcare costs has also been established [7]. The extensive use and reliance upon smartphones for healthcare, however, poses certain risks [8]. There are over 43,000 apps on the iOS App Store alone and according to the Food and Drug Administration (FDA) mobile health (mHealth) apps were downloaded by 660 million people as of June 2013 [9].

There are thousands of mobile healthcare apps and about 40% of them are directly related to patient health and treatment [10], and these apps are not regulated by the FDA or any other agency. Android apps require no approval at all [11] and any developer can upload their healthcare apps on the global market. This poses many risks to the privacy and security of the app users [12] but it can also cause physical harm by providing misleading information and poorly developed features. Research has demonstrated that many medical applications currently available in mobile app stores have flaws that could prove detrimental for medical practitioners and their patients [13]. Considerations when choosing an app include ensuring that the information found within is complete and accurate, that the app is stable and adequately supported, and that safety mechanisms for data management are in place [13-15]. There are numerous calls for better regulation of healthcare apps [16-18], yet not much has been done to address these concerns.

The wide variety of mHealth apps makes it easy for hackers and individuals with malicious intentions to take advantage of and even harm smartphone users [19]. Developing a taxonomy can help us better understand the purpose of mHealth apps. By grouping apps into categories we can more appropriately address the risks they have in common. To develop the taxonomy, we applied the security challenges in a mobile healthcare environment defined by [20] and we adopted the threat taxonomy for mHealth privacy proposed by [21]. To classify the types of mHealth apps we used the categorization proposed by [4]. These separate tools helped us design an artifact with a much broader perspective, encompassing types of health apps and the security and privacy concerns related to them.

The current study contributes to literature as it expands existing theories on mHealth privacy and security. The proposed artifact is consistent with design science research methods proposed by [22]. The taxonomy has been tested with various types of mobile healthcare applications and it successfully differentiated the risks posed to each app. In addition, the artifact demonstrated value to the user according to the criteria developed by [23].

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.385

IEEE computer society

## 2. Research Questions

The vast number of health apps for various mobile platforms (iOS, Android, Microsoft Mobile, BlackBerry, and Symbian) makes it extremely challenging to develop a unified classification method incorporating the specifics of each system. There are differences in terms of the app approval process, costs for download, app purpose, integration of healthcare sensors, etc. That is why it is important to answer the question: *How can mHealth apps be classified and categorized?* For the purposes of this study, we are using the four dimensions of mobile apps proposed by [4]: (1) patient care and monitoring; (2) health apps for the layperson; (3) communication, education, and research; and (4) physician or student reference apps.

Next, we consider the various types of threats mobile apps are posing to users. Some of the most common threats defined by [21] include: (1) Identity threats: misuse of patient identity information (PII); (2) Access threats: unauthorized access to personal health information (PHI) or personal health records (PHR); and (3) Disclosure threats: unauthorized disclosure of PII or PHI.

These threats are explicitly related to the privacy concerns of mHealth. The problem of mHealth security has been addressed previously [20], but there is a lack of sufficient understanding on how this knowledge can be integrated to classify mHealth apps. Thus, our second research question is: *What are the security and privacy threats for mHealth apps?*

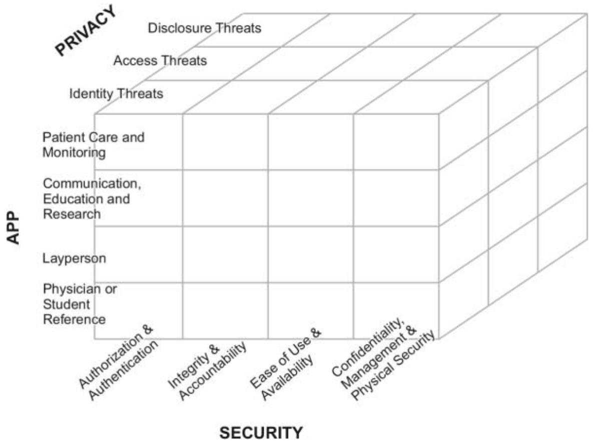
After we outline the possible categories of mHealth apps and the security and privacy threats, our next research question is: *How can mHealth apps be further classified based on the security and privacy threats?* This is important to consider because it will help us build the design science artifact. Establishing a solid connection between the types of mHealth apps and the security and privacy concerns related to them will be beneficial for both practitioners and researchers, and it will shed light on the emerging field of mobile healthcare and risks associated with it.

## 3. Taxonomy Development

We draw upon concepts and theories from prior literature to create a visual representation of the classification dimensions. Following the design science research cycles proposed by [24], the current study attempts to answer the calls for systemizing the vast number of healthcare apps.

In this study, people are the contextual environment and the artifact strives to propose a solution to their problems by doing an analysis of the needs and requirements as stated in prior literature. We refer to the existing knowledge base of healthcare, mobile applications, security, and privacy to create the taxonomy dimensions. After building the artifact, we evaluate it to ensure it has value to end-users as suggested by [23]. We also draw upon the notion that the researcher-practitioner collaboration is key to user adoption and buy-in [25]. We made several iterations of the artifact to ensure it is of high quality and meets user needs. The taxonomy of mHealth apps with respect to security and privacy has three main dimensions, with several subcategories (Figure 1).

**Figure 1. A Three-dimensional Model for Classifying mHealth Apps in Terms of Security and Privacy Concerns**


PRIVACY
Disclosure Threats
Access Threats
Identity Threats
Patient Care and Monitoring
Communication, Education and Research
Layperson
Physician or Student Reference
APP
Authorization & Authentication
Integrity & Accountability
Ease of Use & Availability
Confidentiality, Management & Physical Security
SECURITY

### 3.1. mHealth App Dimension

When designing the mHealth app dimension, we refer to a classification developed by [4]. Following are the four categories they propose.

*Patient care and monitoring* (PCM) – these apps acknowledge the possibility of observing patients via mobile devices. Examples from prior literature include: Android app iWander for patients with Alzheimer disease using a GPS to track their location; smartphones connected via Bluetooth to a single-lead electrocardiograph (ECG) device for patients who are unable to attend traditional hospital-based rehabilitation; and patient self-monitoring – using sensors to record data and promote physical activity.

*Health apps for the layperson (LAY)* – the authors did not find sufficient evidence of trends of patient apps and the ones dedicated to the layperson mostly relate to wellness. Some examples of such apps are: weight loss apps such as Lose It! and Calorie Counter. Using the built-in GPS and accelerometer, smartphones can be turned into navigators and pedometers. There are also apps like iTriage, providing patients with information about the locations of nearby emergency rooms, doctors by specialty, and other practical information.

*Communication, education, and research* (CER) – these are critical applications of smartphones, as they allow users to receive information in a timely manner and be more efficient. There are numerous ways in which mobile apps can be used for communication, education, and research. Some of these are: integration with electronic records, documenting medical evidence for telediagnostics, data on disease outbreaks by location, and data collection during medical trials.

*Physician or student reference apps (REF)* – the authors provide limited evidence of this type of app. However, certain apps can potentially improve the clinical decision making process and reduce medical errors. For example, Anesthesiology i-pocketcards is a clinical reference guide with a compilation of scores, classification, algorithm, and dosage information necessary for the Anesthetics environment. Another reference app is Heart Pro. It is intended for students and medical professionals; it uses real 3D and allows users to observe the heart from any angle.

## 3.2. mHealth Security Dimension

We used the security challenges of the mobile healthcare environment outlined by [20] to create the security dimension of the taxonomy. We shifted the focus from information systems to mobile apps to provide a more relevant context to the current study. We grouped the security challenges into the following four categories based on their definitions and relationships:

- Authentication and Authorization (AA);
- Integrity and Accountability (IA);
- Ease of Use and Availability (EUA);
- Confidentiality, Management, and Physical Security (CMPS)

*Authentication* – Proof of identity is an essential component of any app that handles confidential information, as by implementing authentication techniques we can distinguish legitimate users from imposters.

*Authorization* – Authorization and authentication are two related concepts. Authorization is the act of determining whether a particular user has the right to carry out a certain activity, such as reading/writing to a file. After the user is authenticated depending on their credentials, they get access to a particular view of the app.

*Accountability* – Identifies that in the case of misuse by an individual, the user can be tracked down and answer for their actions to the appropriate authority.

*Integrity* – Information may be altered when it is exchanged in an insecure network, resulting potentially in many problems. The consequences of using inaccurate information can be disastrous. If improperly modified, data could become useless, or worse, dangerous.

*Availability* – Mobile apps can become inaccessible at a given time, resulting in loss of availability. This means people who are authorized to get information cannot get what they need. Loss of availability can have severe consequences for users who rely on the app for decision-making.

*Ease of use* – The security component must be easy to use, else users will switch security off or bypass. Users usually do not want complex security that will slow down their tasks; if possible, the security functions should be invisible to the end user.

*Confidentiality* – Ensures that information is available only to those who are authorized to access it. Many healthcare apps require information confidentiality in order to protect the data of the patients.

*Management* – All apps must be properly managed to ensure the normal flow of operation and information involved. The administrator should maintain procedures to inspect at frequent intervals the operation of the app to determine if any activity is problematic and take appropriate actions.

*Physical security* – Physical security plays an important role in attaining the security of the mobile device as well as the back-end datacenter used by the app developer. There is risk inherent in any data-collecting app on a smartphone if the device is stolen, but mHealth apps include particularly sensitive information about the device owner.

## 3.3. mHealth Privacy Dimension

We used the privacy-related threats in mHealth systems [21] to design the privacy dimension of the taxonomy.

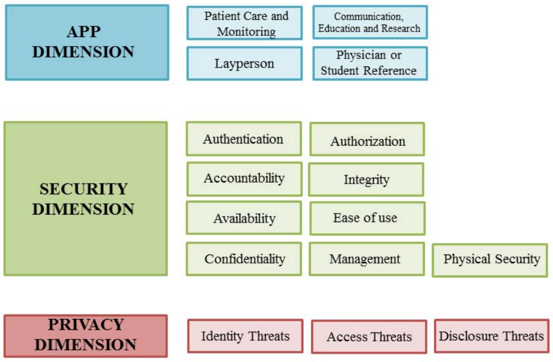
*Identity threats (ID)* – these are related to patients losing or sharing their identity credentials, thus enabling others to access their PHR. Also, insiders may use the credentials for medical fraud, potentially with financial or medical damage to the patient. In some settings although patient identities are removed from files, an outsider may re-identify them with another data source.

*Access threats (ACC)* – since patients have ultimate control on the collection, use, and disclosure of PHI, if they fail to express their consent, broader-than-intended access can be granted. Another threat is that insiders may share patient data leading to expensive legal ramifications. Modifying health records is another problem, whether it is intentional or unintentional.

*Disclosure threats (DIS)* – these are related to several factors. First, secure data transmission requires covered entities to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Second, the device presence is concerned with leaking patient data about the location or sensor type of the patients. And third, device compromise or theft poses risks to releasing PHI, information about the sensors patients are using, and their medical condition. To many of these concerns there are no complete solutions existing yet.

Figure 2 represents the dimensions of the proposed taxonomy and summarizes the discussed ideas:

**Figure 2. A Taxonomy of mHealth Apps – Security and Privacy Concerns**



## 4. Method

To evaluate the taxonomy and further illustrate its usefulness to the study of design of mHealth apps, we followed a methodology proposed by [24].

We used the report created by the IMS Institute for Healthcare Informatics [26] to identify exemplar apps. We referred to the list of top healthcare apps identified in the paper (p. 23-27) and we evaluated our taxonomy against those top-rated apps. We classified all apps on which we were able to find information, and we had a total of 38 apps to review.

We followed quantitative content analysis methods [27] to improve the quality of the study. We chose to combine this research method with Hevner's [22] recommendations on evaluating design science artifacts because it provides a high degree of transparency and its flexibility allows us to successfully apply it to the content of mHealth applications.

To ensure the reliability of the results two researchers independently evaluated the taxonomy against the list of top-rated apps. Before the evaluation process, they developed a coding schedule in which all data relating to an item being coded was entered. To avoid any inter-coder reliability issues, the researchers evaluated one of the apps together. Thus they were able to better understand the classification method and reach consensus on the level of relevance of the apps to the taxonomy dimensions. At the end they compared ratings and agreed on the classification of each app collaboratively.

We explored the iOS App and Google Play stores for mobile apps to find more information on the top-rated applications outlined by [26] and categorize the apps according to our proposed classification. We referred to the app descriptions and screenshots provided by developers to understand how each category applies to each healthcare app. We were able to distinguish three levels of relevance of the apps on each of the taxonomy dimensions: none, partial, and full relevance. We evaluated the proper category of healthcare app as well as the extent to which the app addressed basic security and privacy dimensions.

In addition to the three dimensions of the taxonomy, the mHealth apps can be also defined into other categories, such as:

- Type of institution (hospitals, insurance companies, pharmacies, banks);
- Type of service (medical or dental);
- Type of wellness (healthy eating, fitness, sport, stress, meditation);
- Type of disease (diabetes, heart problems, allergies).

These examples can be used to further enhance the three main dimensions already identified in the taxonomy. Since this is an exploratory study, it is beyond its scope to drill down into these new categories. Rather, our goal is to start a discussion on how personal health data is managed and how individual privacy is guaranteed when using mHealth apps.

## 5. Results

Results of the evaluation of the taxonomy provide support for its usefulness and utility. We were able to successfully categorize 38 top-rated mHealth apps. To better visualize the results of the evaluation, we coded each app using the three established relevancy indicators (none, partial, full). Results are presented by demonstrating how the classification method can be applied to three apps. Evaluation of the full list of

38 top-rated mHealth apps is provided in Appendix A.

### 5.1. Healow by eClinicalWorks

Healow (Figure 3) is a mobile app for communication between patients and doctors and it provides patients access to their up to date health records. Patients can also access their appointments, lab results, vitals; manage medications and other personal health data. Patients can manage multiple accounts of them and their families. The app can be used for weight management, to track progress, to set goals, etc.

Based on that information, we classified the app to have full relevance on the following health app dimensions:

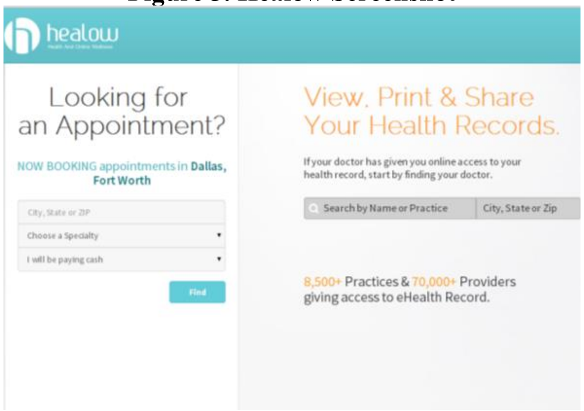
- patient care and monitoring (PCM);
- communication, education and research (CER);
- layperson (LAY).

The app, however, has no direct value as a physician or student reference, as it does not provide any specific information for improving clinical decision making.

In terms of security, Healow requires login information and stores patient data. The integrity and accountability of the data are also crucial. Significant management on the back end from the physicians' healthcare practices is also required. Thus, we classify Healow to have full relevance on all four security dimensions (AA, IA, EUA, and CMPS).

Based on the detailed personal information collected and exchanged via Healow, we can classify it to also have full relevance on the access (ACC), identity (ID), and disclosure (DIS) privacy dimensions.

**Figure 3. Healow Screenshot**



Looking for an Appointment?

NOW BOOKING appointments in Dallas, Fort Worth

View, Print & Share Your Health Records.

If your doctor has given you online access to your health record, start by finding your doctor.

8,500+ Practices & 70,000+ Providers giving access to eHealth Record.

### 5.2. WebMD for iPad by WebMD

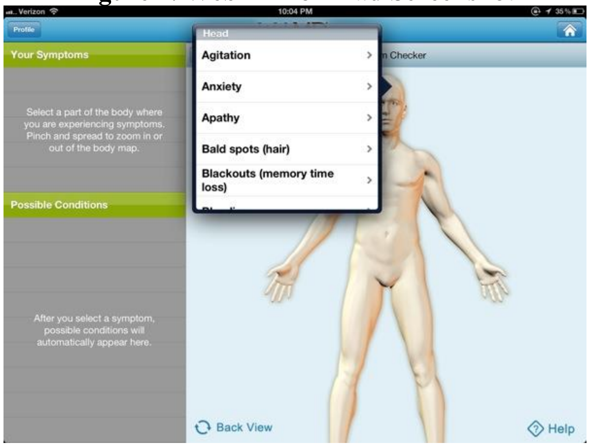
WebMD for iPad (Figure 4) is a companion app to the very popular self-diagnosis information website. Patients can input symptoms into the app and receive a list of possible conditions. For each condition, extensive background education is provided. Additionally, life-saving tips, such as a CPR procedure, are included with illustrations. The app also provides a comprehensive database of drugs that can educate patients on side effects and potentially hazardous interactions between medications.

Using our taxonomy, we categorized the app as being fully relevant to the layperson (LAY) as well as a communication, education, and research (CER) type of app. Because of its extensive drug database and comprehensive symptom/condition evaluation engine, we considered it partially relevant as a physician or student reference (REF).

The app has an optional ability to link with an online WebMD account to import information. For that reason, we found it partially relevant for most of the security dimensions. Since the valuable information in the app is available without a login and even when offline, we considered it fully relevant for integrity and availability (IA).

Due to the optional nature of the login to the back-end WebMD database, we considered all three access, identity, and disclosure privacy dimensions as partially relevant.

**Figure 4. WebMD for iPad Screenshot**



Select a part of the body where you are experiencing symptoms. Pinch and spread to zoom in or out of the body map.

After you select a symptom, possible conditions will automatically appear here.

### 5.3. Zimmer Arthritis 411 by Zimmer

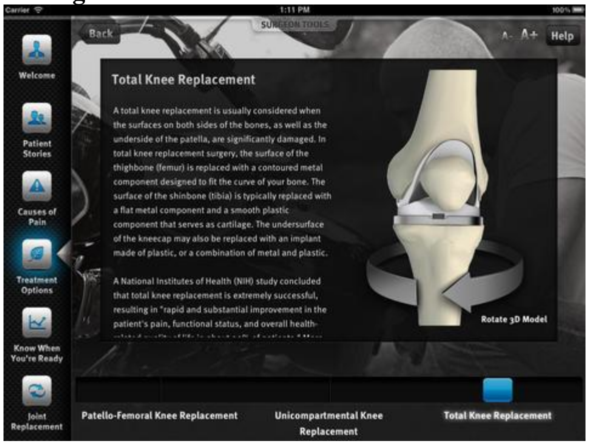
The Zimmer Arthritis 411 app (Figure 5) is the only one in the study sample that is intended to be used in direct conjunction with the physician, as opposed to apps that aim to stand in when the physician is not available. Replacing literature pamphlets that were previously given to patients, the app allows the surgeon to explain in great detail the surgical procedures to patients with diagrams, videos, and interactivity that can reduce anxiety. This education can begin during a consultation at the doctor's office and the patient can later refer to the diagrams and educational material in the comfort of their own homes.

We categorized this app as fully relevant to the layperson (LAY) and partially relevant to communication, education, and research (CER), and physician and student reference (REF). The app was not relevant to ongoing patient care and monitoring (PCM) because it was meant only in an education capacity.

Because the app does not require a login to a back-end provider system, there are no authorization and authentication (AA), or confidentiality, management, and physical security (CMPS) concerns. The integrity and accountability (IA) of the app are maintained because the information cannot be modified. The app provides information even while offline, so ease of use and availability (EUA) are partially relevant.

We scored this app as having no relevance to any of the three privacy dimensions because no personal information is recorded in the app. Therefore, there are no disclosure (DIS), access (ACC), or identity (ID) issues associated with the data in the app.

**Figure 5. Zimmer Arthritis 411 Screenshot**



Total Knee Replacement

A total knee replacement is usually considered when the surfaces on both sides of the bones, as well as the underside of the patella, are significantly damaged. In total knee replacement surgery, the surface of the thighbone (femur) is replaced with a contoured metal component designed to fit the curve of your bone. The surface of the shinbone (tibia) is typically replaced with a flat metal component and a smooth plastic component that serves as cartilage. The undersurface of the kneecap may also be replaced with an implant made of plastic, or a combination of metal and plastic.

A National Institutes of Health (NIH) study concluded that total knee replacement is extremely successful, resulting in "rapid and substantial improvement in the patient's pain, functional status, and overall health-

Results from these classifications suggest that having a unified taxonomy to categorize mHealth apps is useful and necessary. Especially due to the essence of the collected data, addressing the privacy and security issues is of key significance. Disappointingly, during the data collection process we discovered that most app descriptions and reviews were concerned with the user experience and ease of use of the application, rather than discussing the use, storage, and access to patients' data. This is a potential issue because there are certain rules and regulations about managing health data, such as HIPAA and the HITECH Act. These acts are not yet widely applied in mHealth apps and many of the app installation agreements indicate personal data can be used for marketing purposes or sold to third parties. The increasing amounts of mobile-generated data create a potential problem for patient security and privacy that needs to be addressed by legislators and then reflected in the development of mobile apps.

Further, results of the data analysis outline the potential of the proposed taxonomy to encompass a wide variety of mHealth apps and classify them based on the security and privacy dimensions described earlier. The classification of each app demonstrates how the artifact we developed can be successfully utilized by both developers and end users. The taxonomy achieved its goal to answer the research questions and to provide more relevancy to the problem of mobile healthcare security and privacy.

## 6. Discussion

There are several practical implications from this study. First, there are currently no explicit regulations to assess the types of mHealth apps being published. This taxonomy aims to raise awareness for the problem of collecting and managing health data from mobile users. The lack of regulation on the mobile market poses a potential threat to the privacy and security of data obtained from mHealth applications. Users often install a large number of apps from unfamiliar brands without reading the app developers' privacy policies. One solution to this problem can be augmenting centralized markets with information about trusted brands and trusted application reviewers [28]. Our study confirms these previous findings and we think centralized markets can be a viable solution to address the privacy and security issues of mHealth apps. Because of the large number of existing apps on the market, however, it may be difficult to force developers to change their processes and adopt new policies for addressing mHealth security and privacy issues.

A second implication of this study for practice is the need to specifically address the privacy and security concerns when providing descriptions and screenshots of apps in the app stores. We observed many inconsistencies when searching for apps to evaluate the taxonomy. One of our findings is that keywords in app descriptions are used for search optimization rather than to provide users with detailed information about the risks each app poses. Oftentimes only after downloading the app, the user has access to the privacy policies and terms of use. [29] present the idea that reading such notices is related to concerns for privacy, positive perceptions about notice comprehension, and higher levels of trust in the notice. Further, the authors find that reading privacy notices is only one element in the overall strategy consumers use to manage the risks of disclosing personal information online (p.15). The problem of privacy self-management is becoming more and more important [30] which leads users to the dilemma of choosing between their privacy and the need to use a mHealth app. In this study, our goal was to start a discussion on this important topic and suggest ways to make mHealth apps useful without making sacrifices on users' privacy and security.

Based on our data analysis, we can infer that a variety of mobile apps exist on the market and they address the needs of both patients and physicians. The proposed taxonomy provides answers to the three research questions, as it demonstrates in practice how mHealth security and privacy concerns can be successfully defined and classified. Further, our findings suggest that such an integrated approach can be adopted by the development community and can lead to decrease in privacy and security threats to end users. Our sample encompasses a wide variety of mHealth applications, as our goal is to test the utility of the taxonomy with as many different applications as possible. Further, our results support the concept that mHealth apps can, in fact, be classified based on their level of security and privacy and how these concerns are related to healthcare data. The three applications we discussed into more detail are a representative sample of the vast number of mHealth apps and provide valuable insights as how the taxonomy is relevant to the needs and concerns of end users regarding their privacy and security.

This is an exploratory study and further research needs to be done to examine into more detail the dimensions of the taxonomy, which can be broken into various subcategories. However, this study is more focused on developing high-level concepts to organize the vast number of mHealth apps available to users. We encourage others to explore different venues to approach the problem. Another option to test the taxonomy is by conducting experiments with users. They can be exposed to the different categories of apps and researchers can measure users' perception of privacy and security issues for each app. Thus, a correlation between the ranking of apps and the perceived concerns can be explored.

## 7. Conclusions

The current study focuses on the important problems associated with the use of mHealth apps. Although some providers give terms of use and privacy policies when downloading the app, there is not yet an adequate or a unified way to provide such information in the app stores. Developers rely on key words and attractive phrases to improve search engine optimization and encourage users to download their apps. Even after a health app is being installed, it is sometimes not clear how data are managed and who has access to them.

The proposed taxonomy creates a model of capturing the most important features of mHealth apps with respect to privacy and security. We categorized a list of 38 top rated apps to test and evaluate our artifact. Although there are many existing healthcare applications, the proposed dimensions can successfully classify them and compare them against each criterion.

This study contributes to literature in two aspects. First, it builds upon prior research and applies the concerns of privacy and security to mHealth applications. Expanding on previous studies is crucial, as it helps us apply the most important aspects to create the three dimensions – type of apps, security, and privacy concerns. These three have proven to be stable and necessary perceptions of mHealth apps over time and including them into a single framework is logical and creates coherence. Second, mobile healthcare is still a relatively recent and undeveloped area of research. Thus, adding more knowledge to the domain creates a potential avenue for further research and sheds more light on a problem that is of increasing value.

## 8. References

[1] Boulos, M.N., Wheeler, S., Tavares, C., and Jones, R., "How Smartphones Are Changing the Face of Mobile and Participatory Healthcare: An Overview, with Example from Ecaalyx", Biomedical engineering online, 10(1), 2011, pp. 24.

[2] Park, Y., and Chen, J.V., "Acceptance and Adoption of the Innovative Use of Smartphone", Industrial Management & Data Systems, 107(9), 2007, pp. 1349-1365.

[3] Burdette, S.D., Herchline, T.E., and Oehler, R., "Practicing Medicine in a Technological Age: Using Smartphones in Clinical Practice", Clinical infectious diseases, 47(1), 2008, pp. 117-122.

[4] Ozdalga, E., Ozdalga, A., and Ahuja, N., "The Smartphone in Medicine: A Review of Current and Potential Use among Physicians and Students", Journal of medical Internet research, 14(5), 2012,

[5] Luxton, D.D., Mccann, R.A., Bush, N.E., Mishkind, M.C., and Reger, G.M., "Mhealth for Mental Health: Integrating Smartphone Technology in Behavioral Healthcare", Professional Psychology: Research and Practice, 42(6), 2011, pp. 505.

[6] Brennan, P.F., Downs, S., and Casper, G., "Project Healthdesign: Rethinking the Power and Potential of Personal Health Records", Journal of biomedical informatics, 43(5), 2010, pp. S3-S5.

[7] Mobilesmith, I., "Mobile Apps as Tools of Cost Reduction in Healthcare: The Impact of Mobile Apps on

Healthcare Costs", in Mobile Apps as Tools of Cost Reduction in Healthcare: The Impact of Mobile Apps on Healthcare Costs, 2014

[8] Gill, P.S., Kamath, A., and Gill, T.S., "Distraction: An Assessment of Smartphone Usage in Health Care Work Settings", Risk management and healthcare policy, 5(2012, pp. 105.

[9] Conn, J., "No Longer a Novelty, Medical Apps Are Increasingly Valuable to Clinicians and Patients ", in No Longer a Novelty, Medical Apps Are Increasingly Valuable to Clinicians and Patients 2013

[10] Constantino, T., "Ims Health Identifies Opportunities for Mobile Healthcare Apps to Drive Patient Engagement, Enhance Delivery of Care", in Ims Health Identifies Opportunities for Mobile Healthcare Apps to Drive Patient Engagement, Enhance Delivery of Care, Parsippany, NJ, 2013

[11] Meier, R., Professional Android 4 Application Development, John Wiley & Sons, 2012.

[12] Zhou, Y., and Jiang, X., "Dissecting Android Malware: Characterization and Evolution", in Dissecting Android Malware: Characterization and Evolution, IEEE, 2012, pp. 95-109.

[13] Aungst, T., Clauson, K., Misra, S., Lewis, T., and Husain, I., "How to Identify, Assess and Utilise Mobile Medical Applications in Clinical Practice", International journal of clinical practice, 68(2), 2014, pp. 155-162.

[14] Misra, S., Lewis, T.L., and Aungst, T.D., "Medical Application Use and the Need for Further Research and Assessment for Clinical Practice: Creation and Integration of Standards for Best Practice to Alleviate Poor Application Design", JAMA Dermatology, 149(6), 2013, pp. 661-662.

[15] Lewis, T.L., "A Systematic Self-Certification Model for Mobile Medical Apps", Journal of medical Internet research, 15(4), 2013, pp. e89.

[16] Visvanathan, A., Hamilton, A., and Brady, R., "Smartphone Apps in Microbiology—Is Better Regulation Required?", Clinical Microbiology and Infection, 18(7), 2012, pp. E218-E220.

[17] Rosser, B.A., and Eccleston, C., "Smartphone Applications for Pain Management", Journal of telemedicine and telecare, 17(6), 2011, pp. 308-312.

[18] Sherwin-Smith, J., and Pritchard-Jones, R., "Medical Applications: The Future of Regulation", Bulletin of The Royal College of Surgeons of England, 94(1), 2012, pp. 12-13.

[19] Felt, A.P., Finifter, M., Chin, E., Hanna, S., and Wagner, D., "A Survey of Mobile Malware in the Wild", in A Survey of Mobile Malware in the Wild, ACM, 2011, pp. 3-14.

[20] Stavrou, E., and Pitsillides, A., "Security Challenges in a Mobile Healthcare Environment", IWWST'05, 2005, pp. 121.

[21] Kotz, D., "A Threat Taxonomy for Mhealth Privacy", in A Threat Taxonomy for Mhealth Privacy, 2011, pp. 1-6.

[22] Hevner, A., March, S.T., Park, J., and Ram, S., "Design Science in Information Systems Research", MIS Quarterly, 28(1), 2004, pp. 75-105.

[23] Boztepe, S., "User Value: Competing Theories and Models", International journal of design, 1(2), 2007, pp. 55-63.

[24] Hevner, A., and Chatterjee, S., Design Research in Information Systems: Theory and Practice, Springer, 2010.

[25] Österle, H., and Otto, B., "Consortium Research", Business & Information Systems Engineering, 2(5), 2010, pp. 283-293.

[26] Informatics, I.I.F.H., "Patient Apps for Improved Healthcare: From Novelty to Mainstream", in Patient Apps for Improved Healthcare: From Novelty to Mainstream, IMS Institute for Healthcare Informatics, Pasippany, NJ, 2013

[27] Bryman, A., Social Research Methods, Oxford university press, 2012.

[28] Chin, E., Felt, A.P., Sekar, V., and Wagner, D., "Measuring User Confidence in Smartphone Security and Privacy", in Measuring User Confidence in Smartphone Security and Privacy, ACM, 2012, pp. 1.

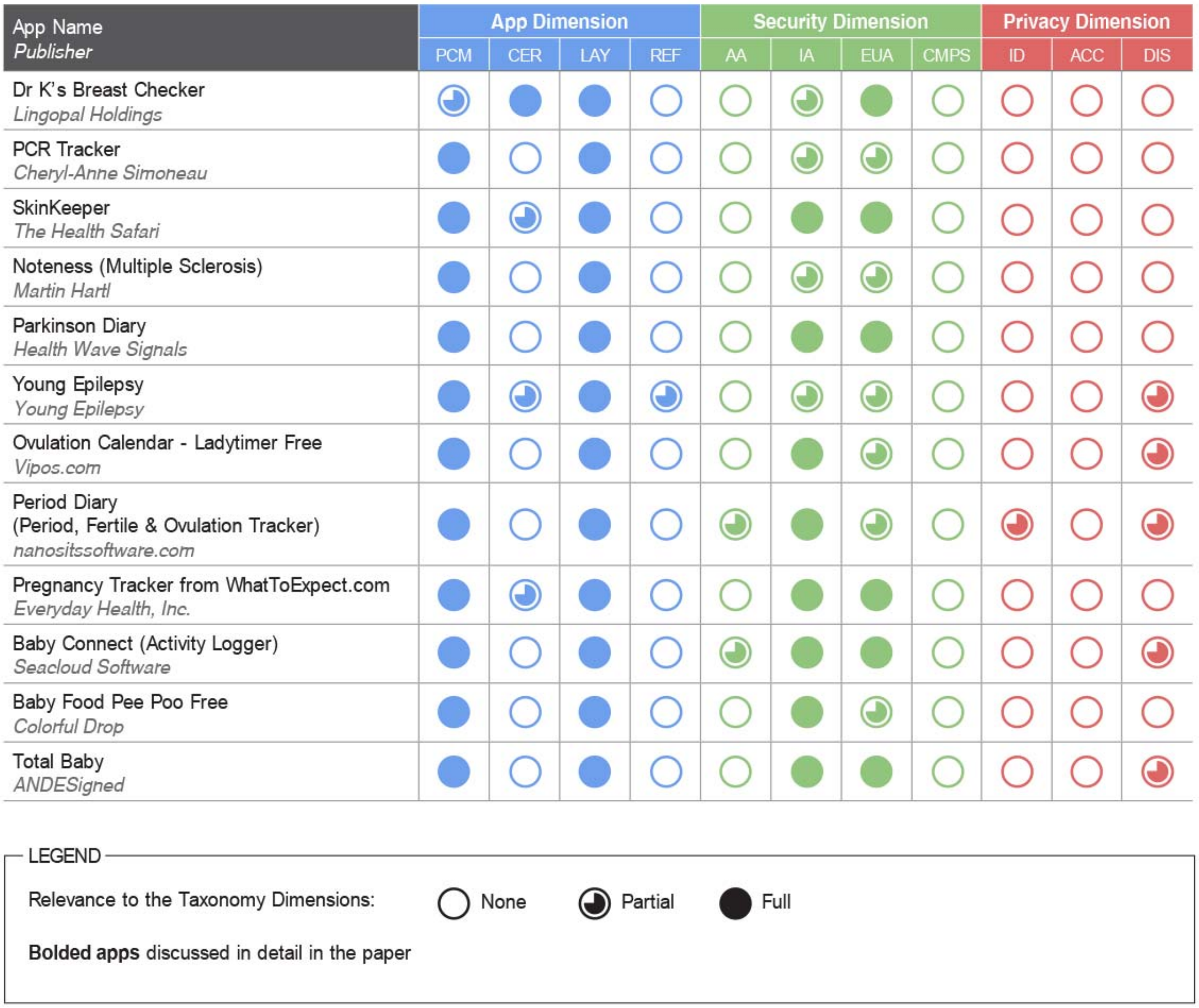
[29] Milne, G.R., and Culnan, M.J., "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", Journal of Interactive Marketing, 18(3), 2004, pp. 15-29.

[30] Solove, D.J., "Introduction: Privacy Self-Management and the Consent Dilemma", 2013,

## Appendix A: Classification of Top-Rated mHealth Apps

| **App Name**<br>*Publisher* | App Dimension | | | | Security Dimension | | | | Privacy Dimension | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | PCM | CER | LAY | REF | AA | IA | EUA | CMPS | ID | ACC | DIS |
| Calorie Counter and Diet Tracker<br>*MyFitnessPal* | ◕ | ◕ | ● | ○ | ◕ | ◕ | ● | ○ | ◕ | ◕ | ◕ |
| Calorie Counter PRO<br>*MyNetDiary* | ◕ | ◕ | ● | ○ | ◕ | ◕ | ● | ○ | ◕ | ◕ | ◕ |
| Chest Trainer: by Fitness Buddy<br>*Azumio* | ○ | ◕ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ |
| Cycle Tracker Pro - TrainingPeaks GPS<br>*Peaksware* | ○ | ○ | ● | ○ | ○ | ● | ● | ◕ | ○ | ◕ | ◕ |
| Quit It 3.0 - stop smoking<br>*Tommy Kammerer* | ○ | ◕ | ● | ○ | ○ | ● | ● | ○ | ○ | ◕ | ◕ |
| Quit Smoking Now HD - Hypnotherapy<br>*Max Kirsten* | ○ | ◕ | ● | ○ | ○ | ● | ● | ○ | ○ | ◕ | ○ |
| **Healow**<br>***eClinicalWorks*** | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● |
| ZocDoc - Doctor Appointments Online!<br>*ZocDoc* | ○ | ● | ● | ○ | ○ | ● | ● | ○ | ◕ | ● | ● |
| HealthTap - free doctor answers to medical and health questions<br>*HealthTap* | ○ | ● | ● | ○ | ◕ | ● | ◕ | ◕ | ◕ | ◕ | ● |
| iTriage<br>*Healthagen* | ○ | ● | ● | ○ | ● | ● | ● | ● | ◕ | ● | ● |
| **WebMD for iPad**<br>***WebMD*** | ○ | ● | ● | ◕ | ◕ | ● | ◕ | ◕ | ◕ | ◕ | ◕ |
| GoodRx<br>*GoodRx* | ○ | ● | ● | ◕ | ○ | ● | ● | ○ | ○ | ◕ | ○ |
| MyRefill Rx<br>*Intelecare Compliance Solutions* | ● | ◕ | ● | ○ | ● | ● | ● | ● | ◕ | ● | ● |
| Walgreens<br>*Walgreen Co.* | ◕ | ◕ | ● | ○ | ● | ● | ● | ● | ● | ◕ | ● |
| Dosecast<br>*Montuno Software* | ◕ | ◕ | ● | ○ | ● | ● | ◕ | ● | ● | ● | ● |
| Pill Monitor Free - Medication Reminders and Logs<br>*Maxwell Software* | ● | ○ | ● | ○ | ○ | ● | ◕ | ○ | ◕ | ○ | ◕ |
| RxmindMe Prescription / Medicine Reminder and Pill Tracker<br>*RxmindMe* | ◕ | ◕ | ● | ○ | ○ | ● | ◕ | ○ | ◕ | ○ | ◕ |
| Daily Carb - Carbohydrate, Glucose, Medication, Blood Pressure and Exercise Tracker<br>*Maxwell Software* | ◕ | ○ | ● | ○ | ● | ● | ● | ◕ | ◕ | ◕ | ◕ |
| Glucose Buddy - Diabetes Logbook Manager w/syncing, Blood Pressure, Weight Tracking<br>*Azumio* | ● | ◕ | ● | ○ | ● | ● | ◕ | ● | ● | ● | ● |
| GoMeals<br>*Sanofi-Aventis U.S.* | ● | ◕ | ● | ○ | ◕ | ● | ◕ | ◕ | ◕ | ◕ | ◕ |
| ADHD Angel<br>*Daniel Anderton* | ● | ● | ● | ○ | ○ | ◕ | ● | ○ | ○ | ○ | ○ |
| Live OCD Free<br>*Pocket Therapist* | ○ | ◕ | ◕ | ○ | ○ | ○ | ◕ | ○ | ○ | ○ | ○ |
| T2 Mood Tracker<br>*The National Center for Telehealth and Technology* | ◕ | ○ | ◕ | ○ | ○ | ◕ | ◕ | ○ | ◕ | ○ | ○ |
| Office-Fit<br>*Medicus 42* | ○ | ◕ | ● | ○ | ○ | ○ | ◕ | ○ | ○ | ○ | ○ |
| WebMD Pain Coach<br>*WebMD* | ◕ | ○ | ● | ○ | ○ | ◕ | ● | ○ | ○ | ○ | ○ |
| **Zimmer Arthritis 411**<br>***Zimmer*** | ○ | ◕ | ● | ◕ | ○ | ● | ◕ | ○ | ○ | ○ | ○ |

## Appendix A: Classification of Top Rated mHealth Apps *(continued)*



| App Name<br>*Publisher* | App Dimension | | | | Security Dimension | | | | Privacy Dimension | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | PCM | CER | LAY | REF | AA | IA | EUA | CMPS | ID | ACC | DIS |
| Dr K's Breast Checker<br>*Lingopal Holdings* | ◕ | ● | ● | ○ | ○ | ◕ | ● | ○ | ○ | ○ | ○ |
| PCR Tracker<br>*Cheryl-Anne Simoneau* | ● | ○ | ● | ○ | ○ | ◕ | ◕ | ○ | ○ | ○ | ○ |
| SkinKeeper<br>*The Health Safari* | ● | ◕ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ |
| Noteness (Multiple Sclerosis)<br>*Martin Hartl* | ● | ○ | ● | ○ | ○ | ◕ | ◕ | ○ | ○ | ○ | ○ |
| Parkinson Diary<br>*Health Wave Signals* | ● | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ |
| Young Epilepsy<br>*Young Epilepsy* | ● | ◕ | ● | ◕ | ○ | ◕ | ◕ | ○ | ○ | ○ | ◕ |
| Ovulation Calendar - Ladytimer Free<br>*Vipos.com* | ● | ○ | ● | ○ | ○ | ● | ◕ | ○ | ○ | ○ | ◕ |
| Period Diary<br>(Period, Fertile & Ovulation Tracker)<br>*nanositssoftware.com* | ● | ○ | ● | ○ | ◕ | ● | ◕ | ○ | ◕ | ○ | ◕ |
| Pregnancy Tracker from WhatToExpect.com<br>*Everyday Health, Inc.* | ● | ◕ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ |
| Baby Connect (Activity Logger)<br>*Seacloud Software* | ● | ○ | ● | ○ | ◕ | ● | ● | ○ | ○ | ○ | ◕ |
| Baby Food Pee Poo Free<br>*Colorful Drop* | ● | ○ | ● | ○ | ○ | ● | ◕ | ○ | ○ | ○ | ○ |
| Total Baby<br>*ANDESigned* | ● | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ◕ |

LEGEND

Relevance to the Taxonomy Dimensions: ○ None ◕ Partial ● Full

**Bolded apps** discussed in detail in the paper