A Review and Comparative Analysis of Security Risks and Safety Measures of Mobile Health Apps

Karen Scott
The Children's Hospital at Westmead
University of Sydney
karen.scott@health.nsw.gov.au

Deborah Richards
Macquarie University
deborah.richards@mq.edu.au

Rajindra Adhikari
Macquarie University
rajindra.adhikari@students.mq.edu.au

Abstract

In line with a patient-centred model of healthcare, Mobile Health applications (mHealth apps) provide convenient and equitable access to health and well-being resources and programs that can enable consumers to monitor their health related problems, understand specific medical conditions and attain personal fitness goals. This increase in access and control comes with an increase in risk and responsibility to identify and manage the associated risks, such as the privacy and security of consumers' personal and health information. Based on a review of the literature, this paper identifies a set of risk and safety features for evaluating mHealth apps and uses those features to conduct a comparative analysis of the 20 most popular mHealth apps. The comparative analysis reveals that current mHealth apps do pose a risk to consumers. To address the safety and privacy concerns, recommendations to consumers and app developers are offered together with consideration of mHealth app future trends.

Keywords: mHealth, security, privacy, Apps.

1 Introduction

Mobile health (mHealth) is the provision of health services and information via mobile devices, such as smartphones, tablet and laptop computers, and personal digital assistants (PDAs) (Akter et al. 2011). mHealth can enable healthcare that is "more accessible, affordable and available" (Akter et al. 2013 p. 181), given that the majority of people throughout the world (more than 5.5 billion people) own a mobile phone (Akter et al. 2013) and their tendency to keep them close at hand at all times (Klasnja and Pratt 2012). mHealth also enables healthcare communication, such as phoning new mothers (Tamrat and Kachnowski 2012) or sending patients an SMS with information about their medical condition (Technologies 2014).

Mobile health applications (health apps) are software programs that offer health-associated facilities for mobile phones and tablet computers (Remedy Health Media 2014). The use of health apps has exploded with the introduction of the smartphone, including Apple's iPhone and Google's Android platform (Schulke 2013). Health apps are available to consumers to use anywhere and anytime, such as while they are at home, at work, studying or travelling (Tech-Target 2009-2014).

Health apps have been integrated into the field of health care in an attempt to address a wide variety of issues. Health apps can significantly improve the availability and affordability of healthcare for patients, especially those in rural and remote locations (Mirza et al. 2008). They can reduce physical and scheduling difficulties between healthcare specialists and patients living in dispersed locations, and help patients interact with healthcare providers (HealthCareBusinessTech 2014). Health apps can enable physicians to keep track of a patient's condition remotely (Brookings 2013, Supplemental Health Care 2014) and assist consumers to

self-monitor their own condition by measuring and collecting personal data, such as food intake, exercise and blood sugar levels (UCSF 2012).

Despite these promised benefits, there are some limitations. Consumers may not have smartphones or may not fully understand how to use them and may be unable to use an app if one is recommended to them (WebMD LLC 1994 - 2014). Incorrect medical advice provided by health apps can be harmful because consumers may rely on the apps to diagnose a condition or delay seeking necessary care (Schulke 2013). Health apps that provide false clinical measurements can lead to inaccurate or unnecessary care for consumers, which could potentially prove fatal. Prior to the existence of mHealth apps, software in general was identified as being responsible for 20% of medication errors (Hicks 2004), with particular concerns around the lack of regulation and policy for regulating safety-critical healthcare applications. Even if regulations existed, "it is an overwhelmingly difficult task for the client to keep up with all regulations manually, and to check if the provider is meeting the compliance" (Khan and Bai (2013, p. 719).

Additionally, health apps may pose significant risks to the privacy and security of consumers' protected health information. Sensitive data gathered by health apps may be accessible to the patient, physician, family or scientific researchers, but may also be shared with third parties, such as advertisers (Vodafone Group 2013), putting the confidentiality of consumers' data at risk. Given the increasing use of electronic health records (EHR) and electronic healthcare (eHealth), the confidentiality, integrity and availability of consumer data are today's major issues for health service providers in terms of security and data privacy (Wang et al. 2013).

The research scope for this project focuses on the data privacy and security issues associated with consumer use of health apps. The research questions are:

1. *What issues related to data privacy and security are involved in using health apps?*
2. *What data privacy and security measures can be used in health apps?*
3. *What is the risk or safety status of current health apps?*
4. *What recommendations can be made to improve the privacy and security of health apps?*

To identify the data privacy and security issues (Question 1) and measures in use (Question 2), we conducted a review of the literature. To understand whether current health apps adhere to the measures or pose a risk (Question 3), we analysed the 20 most popular health apps from Apple and Google stores, further described in our approach. After presenting our findings, we provide recommendations (Question 4) for consumers and developers and our conclusion.

2 Literature Review

Verasoni's research division, AhHa! Insights, executed a study of mobile application usage in the USA in 2012 (Verasoni 2012). The research reviewed the top 150 applications on Google Android and the top 150 applications on Apple iPhone. Their findings were:

1. Medical apps on such topics as emergency medicine, medications and especially medical references were downloaded more by Android than iPhone users.
2. More sleep and meditation apps were available to iPhone than Android users.
3. When total download numbers were considered, exercise was the most prominent app category across iPhone and Android platforms. This category led the field with 102 (34%) of the top 150 apps. Other categories in the top 150 apps were: medical reference guides with 34 apps (11%), weight loss with 31 (10%), sleep and meditation with 26 (9%), women's health with 21 (7%), medical tools and instruments with 19 (6%), medication with 15 (5%), pregnancy with 14 (5%) and other health apps with 38 (13%).
4. The top earning apps for Android and iPhone users were exercise, weight loss, sleep and meditation, and women's health.

5. Downloads for paid apps were seven times higher for iPhone than Android users.

The increasing number of health apps could improve the quality and affordability of health care and allow patients to safely and securely connect with their physicians. However, Schulke (2013) warns that the increase of free and paid health apps on the market might pose health risks to patients due to a lack of health professional involvement in the development of the apps. Schulke (2013) defines two broad classes of health apps: provider-focused and patient-focused. This literature review considers data privacy and security risks of health apps from a consumer perspective and includes use of a health app by a provider, patient and the general public. We present below a number of security and privacy themes identified from the literature, including security and privacy challenges, poorly protected consumer data, data security breaches, lack of app standards/guidelines and health app cloud storage. Finally, we present suggested security measures for mobile devices to minimise these risks.

2.1 Security and privacy issues

Data security and privacy are major concerns for the use of EHR (Kharrazi et al. 2012) and health apps by healthcare providers and consumers (Ford Faudree and Ford (2013), and pose a major barrier to their widespread use (Kharrazi et al. 2012). If healthcare providers are unable to provide adequate safeguards to patient privacy when accessing EHR from a mobile device, the consequences can be significant. As evidence of the security and privacy challenges, Kharrazi et al. (2012) reported that a small survey found 93% of clinicians use smartphones to access EHR but only 38% follow a formal mobile privacy policy. Kharrazi et al. (2012) also note that individual healthcare providers and consumers may lose their devices or may not use any security authentication to protect their data. Therefore to keep data secure and private, it is the responsibility of individual health professionals and consumers to set up device and app passwords.

Privacy issues related to using health apps include a breach of consumer confidentiality, data privacy shortcomings and security problems. To accelerate adoption of mHealth, it is important for individual apps to put in place supportive privacy policies (P. A. Consulting 2012). A clear privacy policy can tell consumers what permissions an app requires of the device before downloading it, such as geo-location services access, book access, camera access, phone call access and contacts access. If consumers are not comfortable with health apps that are asking many permissions, they should avoid downloading them.

2.2 Poorly protected consumer data

The poor protection of consumer data in health apps has been reported by McCarthy (2013). In the study of 43 health and fitness apps, it was found that only 74% of the free apps and 60% of the paid apps had a privacy policy, available either in the app or on the developer's website. However, only 25% of the free apps and 48% of the paid apps informed consumers about the privacy policy. Furthermore, none of the free apps and only a few of the paid apps encrypted the data that consumers entered into the apps. Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Therefore health apps that do not encrypt consumers' information can pose a threat to data privacy.

Similarly, Nasiri (HealthCareBusinessTech 2014) found the information that consumers entered into health apps may carry privacy risks. He reported a survey of 20 of the 23 most popular free health apps that found 50% send data to third-party advertisers and 39% send data to unidentified parties without any data encryption. He found paid health apps are safer than free health apps to a certain degree and that many free health apps send data, connect to third-party sites, use unencrypted connections, allow for data collection by third parties and store data externally. Most of the time users are not notified that this has occurred. Based on a Clearinghouse review of 43 popular health and fitness apps, Leventhal (2013) concluded that "consumers should not assume any of their data is private in the mobile application environment - even health data that they consider sensitive" Leventhal (2013, p.1).

Some health apps involve an internet-enabled mobile device connecting wirelessly to portable or embedded sensors that track or measure a patient's health condition or a user's activities, which can also pose a security risk (Vodafone Group 2013). The tracking of the user's health can occur in real-time, with or without the user's involvement or approval and can be simultaneously shared with others. The data gathered by such health apps not only carry detailed information about a user's health but also about their habits, location and movements, which can put the user's sensitive information at risk if such information is disclosed.

2.3 Data security breaches

Data security breaches in healthcare have become common, according to Figg and Kam (2011), with many on-line mHealth providers, including doctors and scientific researchers, able to view patients' medical records without patients' knowledge. The authors noted that the data security breaches in healthcare are a privacy threat that might lead to medical identity theft. The World Privacy Forum describe medical identity theft as an occurrence in which a person uses another person's identity, such as a person's name or Medicare number, without the person's knowledge and consent, which would impact many consumers' security (Dixon 2006). According to the US Federal Trade Commission (FTC, 2015), in 2014 identity theft topped the list of consumer complaints for the 15th consecutive year.

Medical identity theft could result in some unauthorized benefits to the offender. The offender may steal patients' records to sell on the black market or alter patients' records for fun, such as adding false entries regarding diagnosis, blood types, drug allergies and other health information. Victims who have their medical records altered by offenders may receive false medical treatment that may have negative consequences to their health, possibly causing death.

2.4 Lack of app standards and guidelines

Exposure to the risks identified above, including fraud and identify theft, unauthorised access to personal information and loss or theft of a mobile device with unencrypted consumer data, need to be monitored and mitigated. A secure mHealth environment that builds trust among consumers and healthcare service providers would need to adopt standard app development guidelines to increase security and protect consumers from any unauthorized attacks (Faudree and Ford 2013). Currently, security concerns about health apps are increasing due to the lack of standard app development guidelines (Kharrazi et al. 2012). Kharrazi et al. (2012) emphasise that a thorough verification process is required by the app stores that could detect unsafe programs and thereby reduce the security risks of health apps.

The problem goes beyond the need for development guidelines to a need for regulation or supervision in the development and publication of mobile apps. Some legislation does exist that could potentially be adapted. For example, the Health Insurance Portability and Accountability Act (HIPAA) seeks to protect the privacy rights of individuals by requiring healthcare providers to obtain consent from individuals prior to any disclosure of data to others. However, HIPAA does not explicitly identify and apply the regulations to the mobile context. Although in some countries, such as the United States of America, there have been initiatives to regulate mobile medical apps since 2011, these initiatives have not been approved, as evidenced in a statement on 6th of September 2013 that the "Food and Drug Administration Safety Innovation Act (FDASIA) wants action on the mobile medical applications guidance" (Jarrin, 2013, p.1). An additional factor for consideration is whether regulations are complied with and how compliance is monitored. Currently, verification of compliance to HIPAA is undertaken by independent auditors (Munro 2013).

2.5 mHealth cloud storage

Mobile cloud computing brings a set of new challenges, especially when it comes to the availability of services and the security and privacy of consumers (Gu and Guirguis 2014). Security issues are critical when a healthcare provider plans to deploy a cloud-based EHR management system because moving patient data to the cloud means patient files are hosted

on the servers of the cloud service provider (Piette et al. 2011). According to Rui and Ling (2010), when moving patient data to the cloud, healthcare providers are exposing information to several external threats because the data is available via the Internet. As this data is subject to the same health insurance privacy and security rules, such as HIPAA, as data stored in any other way, both cloud service providers and healthcare providers must understand the consequences in relation to the privacy risks of consumers' sensitive data: the healthcare provider must guarantee the security of patient data by ensuring that the cloud platform has the needed security mechanisms in place (Research 2013); and it is the cloud provider's responsibility to protect the security and privacy of information by providing the security needed to avoid external attacks to steal or even delete the information.

However, compliance with HIPAA's security requirements is harder in the cloud computing context (Moyle 2013) because the implementation of compliance resides with the cloud provider, while the legal responsibility remains with the healthcare provider. The US Department of Health and Human Services recently modified the HIPAA legislation to include cloud providers in the legal framework under the term Business Associate Agreement (BAA) to specify the legal and financial liabilities of cloud service providers (Munro 2013). Despite this change, due to the common use of third-party providers by cloud providers, data protection agencies in the US and European Union (EU), place ultimate accountability with the clients of cloud computing.

2.6 Mobile device security measures

Mobile technology is the technology used for cellular communication. The US Office of Civil Rights (OCR) recently launched an educational initiative for mobile devices (HealthIt 2014), which identified the following guidelines for app developers: know the risks; take the steps; protect and secure health information. Table 1 summarises measures suggested by OCR (HealthIt 2014; Senft 2013) to ensure mHealth information is secure when using mobile devices such as smartphones and tablets. The OCR has reported that a significant number of data privacy breaches each year arise from lost or stolen mobile devices. With increasing access to unsecured Wi-Fi networks and file sharing features, security is a greater concern as breaches could occur from unauthorized access to data stored on mobile devices (Wikipedia 2014).

Measure	Description
Use of a password or other user authentication	Mobile devices can be configured to require passwords, personal identification numbers (PINs) or passcodes to gain access. These can be masked to prevent people seeing them.
Install & enable encryption	Encryption renders data unusable, unreadable and undecipherable to unauthorized individuals.
Activate remote wiping and/or remote disabling	Remote wiping allows an individual to permanently erase all data stored on a mobile device remotely if the device is lost or stolen. If the mobile device is later recovered, it can be unlocked.
File-sharing applications or software	File sharing allows Internet users to connect and share or trade files. Enabled file sharing could provide unauthorized users with access to a mobile device without users' knowledge.
Firewall	A personal firewall can protect against unauthorized connections by intercepting incoming and outgoing connection attempts and blocking or permitting the connection based on an established predetermined set of rules
Security software	Security software can be installed and regularly updated to protect against malicious applications, viruses, spyware and malware-based attacks, which can exist in email attachments, websites or downloaded programs.
Using non-secured Wi-Fi network or hotspot	Without using a secured Wi-Fi network, there is a risk that communications will be intercepted. Users should avoid sending or receiving information when connected to public wireless network.
Delete mHealth information	All data stored on a mobile device needs to be deleted before the device is discarded. Software can be installed to overwrite the data or devices can purge or destroy the data.

Table 1. Measures to ensure mHealth information is secure (HealthIt 2014) (Senft 2013)

Based on findings from the selected literature, it appears that security and data privacy in health apps are growing concerns among healthcare providers and consumers. The lack of privacy of user data and lack of regulation and guidelines for the development of health apps need to be considered for the improvement of health apps.

3 Methodology

To determine the extent to which current health apps pose a data privacy and security threat and, where necessary, recommend solutions, we conducted a comparative analysis as a case study of the 20 most popular free and paid health apps from Apple and Google stores. The process involved the following three steps:

1. Selection criteria for 20 health apps
2. Identification of data privacy and security features and issues of the 20 health apps
3. Comparative analysis of 20 health apps

The selection of the apps was determined by the highest number of downloads on the health app market, with high ratings from consumers, search engines or app stores, and recommendations through social media. Apps were trialled on appropriate mobile devices: apps from Apple stores on an iPod Touch and apps from Google stores on an android phone.

From the literature we identified a set of nine features, presented in the results section, that we categorised as security risks (first three) or safety measures (last six). To measure each app against these features we asked the questions below. Note question 2 is used to identify risk (i.e. cloud storage) and safety measure (i.e. local storage of data that is password restricted).

1. *Does the app ask for user registration (name, address, birthday and email)?*
   Most health apps available on the market ask for consumers' details prior to registration. It is consumers' responsibility whether or not to provide information to health apps. Providing detailed information may result in compromising data privacy.
2. *Where is data stored (locally on a device or in a cloud)?*
   Data storage is the recording and storing of consumer information. Data storage can either be possible locally on the mobile device or in cloud storage, depending upon the development of the health app.
3. *Is consumer data shared with a third party or advertiser?*
   Sharing of health consumer data with a third party or advertiser is becoming a more serious concern as many apps share consumers' data to generate revenue. Health apps collect detailed personal and health information from consumers to provide better services for health and well-being, but sharing sensitive health information with third parties and advertisers impacts many consumers' data privacy and security.
4. *Does an app ask for user authentication (user name and password)?*
   Some of the most common threats to data security and patient privacy come from unauthorized access. The purpose of the security evaluation is to check security mechanisms (username and password) are implemented to guarantee the privacy of consumers' data.
5. *Are consumers able to update and correct their personal profiles?*
   This allows consumers to change their individual profiles according to the policy of the health apps. Updating patient records improves data accuracy and supports better patient care.
6. *Can consumers delete any personal information completely?*
   It is a prime concern whether health apps allow consumers to delete their personnel information completely. When consumers stop using a health app, they need to be able to delete it. They also need to be able to delete their personal profile and any data archives that have been created with their personal information.
7. *Are consumers informed about any data privacy and security measures?*
   Ensuring the privacy and security of health information, including EHR, is a key component to building the trust required to realize the potential benefits of electronic health information exchange.
8. *Is there a privacy policy?*
   The privacy policy sets out how a health app uses and protects any information that consumers give to app owners when using the health app.

4 Results of Selection Process of 20 Apps

In this section we present the evaluation results of the 20 most used health apps on the market based on their privacy and security features. To conduct the comparative analysis, all 20 apps were downloaded onto a corresponding device (iPhone or Android smartphone). Using the above questions, we analysed each app's authentication functions and features relating to consumer data privacy, as well as the privacy policy on the developers' websites. A description of each app and how it met the selection criteria for inclusion in our evaluation is provided below.

4.1 Apple Stores

MyFitnessPal (MyFitnessPal 2005 - 2014) is an online and app-based wellness-tracking platform, which has a calorie counter and exercise tracker. It helps to evaluate how many calories the user has eaten versus how many they have burnt. The app can also help to track over time any changes, such as weight or waist size. It provides the services for informational purposes only. No medical professionals were involved in its development.

Medscape (Medscape 1994 - 2014), developed by WebMD, is the leading medical resource, mostly used by physicians, medical students, nurses and other health care professionals for clinical information. It supports clinicians with professional tasks, including decision-making at the point-of-care, medical news and professional development. This is the highest rating and fastest growing free health app, with over 4 million registered users.

Epocrates (Epocrates 2014) is the most popular health app among U.S physicians for clinical content and decision support at the point of care. Epocrates has a reliable link of more than a million health care professionals and is used to find providers, review drug prescribing and safety information for thousands of brand and generic medications, and identify pills by imprint code and physical characteristics. The app, built by Epocrates, received the 2ndhighest rating out of 15 apps reviewed by the iMedicalApps Team (iMedicalApps Team 2011).

NeuroMind (DigitalNeurosurgeon 2014) offers interactive clinical decision support. It contains more than 120 clinical classification and grading systems, and some anatomical images for explanation to patients and students. This application has been developed with the involvement of Surgical Neurology International, the European Association of Neurosurgical Societies (EANS), and Neurosurgic.com. It is considered the best app for neurosurgery in the world, with over 200,000 downloads.

Smart Blood Pressure (SmartBP) (Evolve Medical Systems 2012) is an easy-to-use blood pressure management tool that helps patients manage their health using their mobile device. SmartBP allows users to record, analyze and share blood pressure information. It tracks progress and manages blood pressure measurements with an overall goal of improving blood pressure. Blood pressure, pulsing rate and weight can be shared with anyone using email and text message. This application was developed with the involvement of Evolve Medical Systems.

Pill Monitor (Appato 2012) is designed to manage and remind users to take pills on time and at the same time every day, which is good for health. This app is very simple and easy to use. Key features are a schedule for a pill reminder, consumer reminder time, repeat date and dosage of pills, a check of current reminders and upcoming reminders, and a facility that allows users to add photos for each pill. The app was built by Maxwell software and got 4 stars out of 5 based on 353 ratings and 53 user reviews.

Pregnancy & Baby (Apple Inc. 2014) is designed to look at pregnancy phases. Based on the baby's due date, consumers can receive personalized content and get access to the latest parenting news and health information. It also includes a short video of common symptoms and recommendations, and helps consumers to access a variety of online communities. The app was built by Everyday Health Inc. and got 4 stars out of 5 based on 3330 votes.

Diabetes Tracker Plus (Apptism 2013) helps people with diabetes to control blood glucose and stay in good health. Logging and tracking blood sugar using the app supports consumers to self-manage and self-track diabetes. Blood sugar logs and reports can be shared with a healthcare provider by email. There is no information about health professional involvement in the development of the app. This app is recommended by MyNetDiary Diabetes (MyNetDiary Diabetes Inc 2013).

Growth (Clafou Apps 2014) helps to track the growth curves of newborn babies and older children, and compare progress with expected growth rates. This app also helps consumers to share the results with family, friends or health professionals. The development of the app did not involve any health professionals. Growth charts are designed in accordance with and recommended by World Health Organization (WHO) and Centre for Disease Control.

Instant Heart Rate (Azumio 2012) uses iPhones' camera to detect pulse from the fingertip. Prior to using the app, consumers need to place the tip of their finger on the camera for few seconds. A real time chart will show every heartbeat. This app has received the best Health and Fitness app on Mobile Premier Awards 2011. Azumio Inc. was involved in the development of the app and more than 25 million users already use it. There was no health professional involvement in the development of the app.

4.2 Google Store Apps

Ob (Pregnancy) Wheel (Google Play 2014d) is a free android pregnancy calculator. Many clinicians find this app useful, such as those working in primary care, emergency departments and obstetrics. It has numerous adjustable preferences and settings, ultrasound exam dating and dating ordered patient lists. Though developed without professional input, this app is recommended by iMedicalApps Team (iMedicalApps Team 2011) and has got 4.2 stars out of 5 based on 1208 user reviews.

Calorie Counter (Google Play 2014a) is an app to help users find nutritional information about the food they eat and easily keep track of meals. It also counsels patients about diet, exercise and weight. Users are able to look up most types of food, including fast food, supermarket food and pre-prepared food. Consumers can scan barcodes with a camera and the app identifies the type of food, along with allocating the appropriate calories. The app was built by MyFitnessPal, Inc and has got 4.7 stars out of 5 based on 618,588 user reviews.

Skyscape Medical Resources (Google Play 2014f) is a decision support tool that helps physicians, nurses and students to find the right answers of medical resources, such as medical calculators, periodically updated medical news alerts, practice guidelines and disease monographs. More than 2.7 million healthcare professionals access the medical resources in the app. This app is recommended by iMedicalApps Team (iMedicalApps Team 2011).

Endomondo (Google Play 2014b) helps track consumers' workouts and analyze their training. This app can be used as a personal trainer and social fitness partner and is used for running, cycling and walking. It is one of the highest rated apps on the Android market. Though it was developed with health professional input, more than 20 million users are taking advantage of Endomondo app, which has got 4.5 stars out of 5 based 166,459 user reviews.

iTriage (iTriage 2013) is a consumer healthcare company founded in 2008 by two emergency medicine physicians. Over 7 million users have downloaded iTriage app and used it to locate nearby providers based on their symptoms, make appointments, store their personal health record, save medication refill reminders and learn about medications, diseases and procedures. iTriage aims to help answer questions such as: "What medical condition could I have?" and "Where should I go for treatment?

Appointuit (Appointuit 2012) helps consumers make an appointment with doctors anywhere, anytime. This app can also cancel and reschedule an appointment if needed. The Android apps market recommended this app.

Cardiograph (MacroPinch Ltd 2011 - 2013) is used to measure users' heart rate. The app can save results for future reference and keep track of multiple people with individual profiles. It uses a mobile device's built-in camera to take pictures of a user's fingertip and calculate their heart rhythm. The app was built by MacroPinch and has got 4 stars out of 5 based on 61,195 user reviews.

Quit Now (Google Play 2014e) offers real-time stats to help users quit smoking. The indicators tell users how long it has been since they last smoked and the money the user saved. It also shows various indicators for how much the user's heath has improved since they stopped smoking. The app was built by Fewlaps and has 4 stars out of 5 based on 9,780 user reviews.

GI Monitor (Google Play 2014c) is a symptom logging application for patients with IBD (Inflammatory Bowel Disease), Crohn's or Ulcerative Colitis. This app allows patients to log symptoms and provide data to their doctors for optimal treatment. No healthcare personal

were involved in the development of the app. This app is recommended by WellApps, medivo (WellApps 2009 - 2011).

Stress Check (Google Play 2014g) is an app available for quantifying the level of psychological or physical stress. By measuring patient heart rate through the camera and light features on smartphones, Stress Check can estimate the level of stress in real time. The app was built by Azumin Inc. and has got 3.5 stars out of 5 based on 4,223 user reviews.

5 Results: Comparative Analysis

Table 2 shows a summary of the comparative analysis of the 20 mHealth apps, also identifying the extent to which each safety measure or security risk was evident. The results illustrate that not all health apps are free of issues. Out of the 20 apps, only one (5%) enables consumers to delete personal information completely and mentions this facility to users. Over half of the health apps 65% (13/20) asked consumers to enter personal information, such as name, address, email and date of birth, but only two apps asked for consumers' authentication prior to log-in. Half (50%, or 10/20) the apps stored data in a cloud that significantly poses risks to consumers' data privacy and 65% (13/20) of the apps shared consumers' information to a third party or advertisers. Few of the apps (20%, or 4/20) informed consumers about data privacy and security measures, however, 90% (18/20) of the apps have a privacy policy that explained the details of the apps' privacy and security measures.

Even though apps such as "Medscape" and "Skyscape" have higher safety scores (4 out of 6 in Table 2) these apps also have considerably higher risk scores. As shown in Table 2, some apps, such as "Diabetes Tracker Plus" and "Growth," ask users' personal information, such as name, address and email, but do not provide any security authentication, such as username and password, prior to log-in; therefore, such apps potentially put confidentiality of consumers' data at risk. Apps such as "Quit Now", "Pill Monitor" and "Ob Pregnancy" have risk scores of 1 out of 3 but these apps are low risk to use as none asks users for personal information, such as name, address and email, prior to registering the apps.

The apps "NeuroMind", "Smart BP" "Cardiograph" and "Stress Check" apps were found to be relatively safe to use compared to other apps. These apps allow consumers to store results locally on the mobile device and do not share consumer data with a third party or advertisers. Even though none of these apps ask consumers for authentication, such as username and password, to log-in, they are safe to use because they do not require consumers to enter personal information.

Only 20% (4/20) of the apps implement security measures to ensure privacy and security of consumers' information. These involve the use of firewalls, secure connections on websites, frequently the use of secured socket levels (SSL) to encrypt pages that collect user information and security methods such as authentication to determine the identify of registered users, so that appropriate rights and restrictions can be enforced for that user.

	Does the App Ask for User Registration Details	Data Stored In a Cloud	Is Consumer Data Shared With a Third Party or Advertiser	Does an App Ask aor User Authentication (User Name And Password)	Are Consumers Able to Update and Correct Their Personal Profiles	Can Consumers Completely Delete Any Personal Information	Data Stored Locally On a Device	Are Consumers Informed Any Data Privacy and Security Measures	Is There a Privacy Policy	Risk Score Out of 3	Safe Score Out of 6
Myfitnesspal	1	1	1	-	1	1	-	-	1	**3**	**3**
Medscape	1	1	-	1	1	-	-	1	1	**2**	**4**
Epocrates	1	1	1	-	-	-	1	-	1	**3**	**2**
Neuromind	-	-	-	-	-	-	1	-	1	**0**	**2**
Smart Bp	-	-	-	-	-	-	1	-	1	**0**	**2**
Pill Monitor	-	-	1	-	-	-	1	-	-	**1**	**1**
Pregnancy & Baby	1	1	1	1	-	-	1	-	1	**3**	**3**
Diabetes Tracker Plus	1	-	-	-	1	-	1	-	1	**1**	**3**
Growth	1	-	-	-	1	-	1	-	1	**1**	**3**
Instant Heart Rate	1	-	1	-	-	-	1	-	1	**2**	**2**
Ob (Pregnancy)	-	-	1	-	-	-	1	-	-	**1**	**1**
Calorie Counter	1	1	1	-	-	-	-	-	1	**3**	**1**
Skyscape	1	1	1	-	1	-	1	1	1	**3**	**4**
Endomondo	1	1	1	-	-	-	-	-	1	**3**	**1**
Itriage	1	1	1	-	1	-	-	1	1	**3**	**3**
Appointuit	1	1	1	-	1	-	-	1	1	**3**	**3**
Cardiograph	-	-	-	-	-	-	1	-	1	**0**	**2**
Quit Now	-	-	1	-	-	-	1	-	1	**1**	**2**
Gi Monitor	1	1	1	-	1	-	1	-	1	**3**	**3**
Stress Check	-	-	-	-	-	-	1	-	1	**0**	**2**
Total	**13**	**10**	**13**	**2**	**8**	**1**	**14**	**4**	**18**		

Table 2. Health App Comparison Results

6 Discussion

This study aimed to investigate the data security and privacy features of 20 popular free and paid health apps. From our review, it appears the main risks posed to data protection by health apps are lack of information about the app for consumers, insufficient security measures to safeguard consumers' sensitive data, information shared with third party or advertisers and lack of user authentication prior to log-in to the app, such as username and password. We recommend that apps should only collect data that is strictly necessary for the app to perform the desired functionality. We also recommend that app developers include a privacy policy and inform consumers about it. A set of recommendations to consumers and app developers can be found in Table 3.

Consumers	Application developers
Research the app before downloading it	Sensitive consumers' information should always be stored encrypted so attackers cannot retrieve data.
Try to use apps without entering personal information if permitted	Provide user with information about the implementation of security measures and authentication, and what/how/where data is stored.
Look for user reviews and the privacy policy of an app, either through the app store or online.	Include user authentication. Provide options so users can safely retrieve login details if forgotten. Only 10% (2/20) of the apps in our study ask for user authentication prior to log-in.
Remove data when usage stopped. This may prevent unauthorised use of stored data when consumers no longer use the apps.	Minimise sharing information with third parties or advertisers and ask users to confirm agreement before sharing. In our study 65% (13/20) of the apps shared users' information with third parties or advertisers.
Give feedback on product: Users' feedback on the features, privacy and policy, and functions of an app will help the developers to restructure the app appropriately.	Apps should allow consumers to delete their personal information completely. Only 5% (1/20) of the apps in our study mentioned in its privacy policy that consumers can delete information completely; therefore, this criteria needs to be improved appropriately.

Table 3: Recommendations to consumers and app developers

The variety and number of health apps currently available make mHealth an important alternative to traditional face-to-face forms of healthcare. However, as presented in this paper, there are numerous privacy and safety concerns associated with these tools. Nasiri (HealthCareBusinessTech 2014) found that 50% of health apps transfer information to a third party and 39% send data to unidentified parties without consumer consent. In our study of 20 health apps, 65% send consumer data to a third party or advertisers; in a 2013 study of 43 health and fitness apps, only a few of the paid apps encrypted the data entered by consumers (McCarthy 2013). We believe this high rate is due to a lack of appropriate guidelines for app developers and owners.

Furthermore, although 88% (15 out of 17) of the free health apps and 100% (all three) of the paid health apps in our study have a privacy policy, only 23% (4 out of 17) of the free apps and none of the paid apps informed consumers about security measures. The study by McCarthy (2013) found that 74% of free and 60% of paid apps had a privacy policy in the app or on the developer website.

Related to safety, but not evaluated in the apps reviewed here, is the lack of health professional involvement in the development of the health apps, lack of evidence-based medical practices, lack of effectiveness and deficient functionality (Scott et al. 2015). For example, Burke et al (2012, p.3) reported that a small survey conducted in the UK on the ten most popular parenting and child health apps available on iTunes (until that time) showed that only one of the apps had been developed with healthcare professional involvement in the design and evaluation. In addition, Leroux and Rivas (2013, p.1-2) from Stanford University refer to the lack of regulation, effectiveness and evidence-based medical practices in the majority of health apps.

Similarly, McCartney (2013) highlights that users of health apps do not have any source of information to identify which apps provide evidence-based medical content and which do not. She reports that a study in *JAMA Dermatology* found that many apps designed to diagnose melanoma had a failure of 30%. In the United Kingdom the National Health Service (NHS) has

created a database of health apps they have reviewed and approved; however, some of these apps lack real life tests to quantify the potential benefit or harm they contain.

Another issue is related to the lack of independent assessment of the app software before publication. Mack (2013, p 4-5) gives one example of a health app that had to be recalled because the formula used to measure rheumatoid arthritis was wrong. Fortunately the app owner noticed the error and recalled it for a bug fix, accompanied by information to potential users. If there is no independent software verification, it means that several other apps may contain errors and these may provide false results to users.

7 Future Trends for Mobile Health Apps

A study conducted by Rodrigues *et al* (2012), p.167-168) found that the future of mHealth will evolve from individual-focused apps to those that integrate an element of social networking to promote healthy behaviours in groups. Currently, social networking plays a key role within individuals' daily lives and has made a revolution in the way people interact globally. They also note that social network sites, such as Facebook, have health-related support groups that provide educational and emotional support for users (Rodrigues *et al* 2012). The development of mobile health projects that incorporate components of social networking for patients can help endorse group and community health.

In terms of numbers, Walsh (2013, p.1) predicts there will be an explosion in the mHealth market. Mobile Health Trends and Figures 2013-2017 presents the future development of health apps, emphasizing the following eight important trends that will shape the mHealth market until 2017:

1. Smartphone user penetration will be the main driver for the mobile health acceptance;
2. Mobile health applications will be designed specifically for smartphones or tablets;
3. Mobile health applications will be native (developed especially for mobile environment) rather than web-based applications;
4. Lack of regulation is the main market obstacle during the commercialization phase;
5. Customers will continue to drive the market;
6. Applications will adopt traditional health distribution channels;
7. The mHealth market will evolve mainly in countries with high smartphone penetration and health expenditure;
8. Second generation health apps will focus on chronic diseases.

To aid compliance with health regulations, there are efforts to automate the compliance checking through the use of tools and testing suites, such as those developed by the Certification Commission for Health Information Technology (CCHIT) and the National Institute of Standards and Technology (NIST) (Khan and Bai, 2013). An alternative approach has been offered by considering earlier phases of the software development lifecycle to ensure that non-functional requirements, including privacy and security, are elicited from health regulations (Austin et al. 2010; Ingolfo et al. 2011). Work that specifically seeks to provide automated verification of compliance with health regulations in the context of cloud based services and third party service providers has been conducted by Khan and Bai (2013). They address this critical and challenging task by reasoning over regulations that have been transformed into machine-processable language and real-time data from cloud machines on service specific compliance. As Kan and Bai (2103) note, the approach is limited by the relevancy and accuracy of the data they are able to obtain and they are exploring approaches to ensure the data they collect is accurately identified and up to date.

8 Conclusion

This comparative analysis of 20 health apps illustrated that not all health apps available in the app stores are free of privacy and security issues. Major areas that need to be focussed on in order to develop secure apps are standard app development guidelines and security authentication measures, such as device and app passwords, appropriate encryption mechanisms and an informative privacy policy on each app. As future work, it would be important to analyse the security mechanisms and encryption methods of apps. As it is unlikely that vendors will provide this information, discovery of these methods would probably involve trying to hack into an app, a dubious activity that we did not want to undertake. The study seeks to warn consumers, healthcare personal and app developers to take caution when adopting and developing health apps by providing them with the knowledge about app issues, as well as benefits and risk associated with health apps in healthcare.

References

Akter, S., D'Ambra, J., and Ray, P. 2011. "Trustworthiness in Mhealth Information Services: An Assessment of a Hierarchical Model with Mediating and Moderating Effects Using Partial Least Squares (Pls)," *Journal of the American Society for Information Science and Technology* (62:1), pp. 100-116.

Akter, S., D'Ambra, J., and Ray, P. 2013. "Development and Validation of an Instrument to Measure User Perceived Service Quality of Mhealth," *Information & Management* (50:4), pp. 181-195.

Appato. 2012. "Pill Monitor Free- Medication Reminders and Logs." Retrieved 07 - May - 2014, from http://www.appato.com/maxwell-software/pill-monitor-free-medication-reminders-and-logs/#

Apple Inc. 2014. "Pregnancy & Baby What to Expect." Retrieved 09 - May - 2014, from http://itunes.apple.com/au/app/pregnancy-baby-what-to-expect/id289560144?mt=8

Appointuit. 2012. "Appointuit." Retrieved 10 - May - 2014, from http://appointuit.com/why

Apptism. 2013. "Diabetes Tracker Plus Health & Fitness App." Retrieved 09 - May - 2014, from http://www.apptism.com/health-fitness/ooober-inc/diabetes-tracker-plus/

Austin, A., Smith, B., and Williams, L. 2010. "Towards Improved Security Criteria for Certification of Electronic Health Record Systems," *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care*: ACM, pp. 68-73.

Azumio. 2012. "Instatnt Heart Rate." Retrieved 10 - May - 2014, from www.azumio.com/apps/heart-rate/

Brookings, C. f. T. I. a. 2013. "Improving Health Care through Mobile Medical Devices and Sensors." Retrieved 10 - April - 2014, from http://www.brookings.edu/~/media/research/files/papers/2013/10/22%20mobile%20medical%20devices%20west/west_mobile%20medical%20devices_v06.pdf

Clafou Apps. 2014. "Follow Your Child's Growth." Retrieved 10 - May - 2014, from www.growthapp.net

DigitalNeurosurgeon. 2014. "Description." Retrieved 04 - May - 2014, from http://blog.digitalneurosurgeon.com/ & http://itunes.apple.com/us/app/neuromind/id353386909?mt=8

Dixon, P. 2006. "Medical Identity Theft: The Information Crime That Can Kill You," *The world privacy forum*.

Epocrates. 2014. "Epocrates, with You at the Moment of Care." Retrieved 04 - May - 2014, from www.epocrates.com

Evolve Medical Systems. 2012. "Smart Blood Pressure." Retrieved 04 - May - 2014, from http://www.evolvemedsys.com/> and <https://itunes.apple.com/au/app/blood-pressuresmart-blood/id519076558?mt=8

Faudree, B., and Ford, M. 2013. "Security and Privacy in Mobile Health," *CIO Journal*).

Figg, W. C., Ph.D, and Kam, H. J., M.S. 2011. "Medical Information Security," *International journal of Security (IJS)* (5:1).

FTC, 2015. Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014: Imposter Scams on the Rise. *FTC International Monthly*. March 2015. retrieved 9 July 2015 from https://www.ftc.gov/policy/international/ftc-international-monthly/march-2015.

Google Play. 2014a. "Calorie Counter by Fat-Secret." Retrieved 08 - May - 2014, from http://play.google.com/store/apps/details?id=com.fatsecret.android

Google Play. 2014b. "Endomondo Sports Tracker." Retrieved 10 - May - 2014, from http://play.google.com/store/apps/details?id=com.skyscape.android.ui

Google Play. 2014c. "Gi Monitor." Retrieved 12 - May - 2014, from http://play.google.com/store/apps/details?id=com.wellapps.gimonitor

Google Play. 2014d. "Ob Pregnancy Wheel." Retrieved 09 - May - 2014, from http://play.google.com/store/apps/details?id=com.quartertone.medcalc.obwheel

Google Play. 2014e. "Quit Smoking- Quit Now." Retrieved 10 - May - 2014, from http://play.google.com/store/apps/details?id=com.EAGINsoftware.dejaloYa

Google Play. 2014f. "Skyscape Medical Resources." Retrieved 10 - May - 2014, from http://play.google.com/store/apps/details?id=com.skyscape.android.ui

Google Play. 2014g. "Stress Check by Azumio." Retrieved 12 - May - 2014, from http://play.google.com/store/apps/details?id=com.azumio.android.stresscheck

Gu, Q., and Guirguis, M. 2014. "Secure Mobile Cloud Computing and Security Issues," in *High Performance Cloud Auditing and Applications*. Springer, pp. 65-90.

HealthCareBusinessTech. 2014. "Mobile Health Apps Create Privacy Risk, Study Says." Retrieved 18 - March - 2014, from http://www.healthcarebusinesstech.com/mobile-health-apps-privacy/

HealthIt. 2014. "Your Mobile Device and Health Information Privacy and Security." Retrieved 26 - April - 2014, from http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Hicks, R. 2004. *Medmarx 5th Anniversary Data Report: A Chartbook of 2003 Findings and Trends 1999-2003*. US Pharmacopeia.

iMedicalApps Team. 2011. "Top 15 Free Android Medical Apps for Healthcare Professionals." Retrieved 10 - May - 2014, from http://iims.uthscsa.edu/sites/iims/files/Top%2015%20Free%20Android%20Medical%20apps%20for%20Healthcare%20professionals.pdf

Ingolfo, S., Siena, A., and Mylopoulos, J. 2011. "Establishing Regulatory Compliance for Software Requirements," in *Conceptual Modeling–Er 2011*. Springer, pp. 47-61.

iTriage. 2013. "Itriage - Take Charge of Your Health." Retrieved 10 - May - 2014, from https://www.itriagehealth.com/

Jarrin R., 2013. FDASIA Workgroup wants action on mobile medical apps guidance, *mHealth News*, retrieved 9 July 2015 from http://www.mhealthnews.com/news/fdasia-workgroup-wants-action-mobile-medical-apps-guidance.

Khan, K.M., Bai, Y.: 2013. Automatic verification of health regulatory compliance in cloud computing. In: *IEEE 15th International Conference on e-Health Networking, Applications and Services*, pp. 713–717.

Kharrazi, H., Chisholm, R., VanNasdale, D., and Thompson, B. 2012. "Mobile Personal Health Records: An Evaluation of Features and Functionality," *International Journal of Medical Informatics* (81:9), pp. 579-593.

Klasnja, P., and Pratt, W. 2012. "Healthcare in the Pocket: Mapping the Space of Mobile-Phone Health Interventions," *Journal of biomedical informatics* (45:1), pp. 184-198.

Leventhal R. 2013. *Study: popular mobile health apps carry considerable privacy risks.* retrieved 9 February 2015 from: http://www.healthcare-informatics.com/news-item/study-popular-mobile-health-apps-come-considerable-privacy-risks

MacroPinch Ltd. 2011 - 2013. "Cardiograph – Personal Heart Rate Meter." Retrieved 10 - May - 2014, from http://macropinch.com/cardiograph/

McCarthy, M. 2013. "Experts Warn on Data Security in Health and Fitness Apps," *Br. Med. J* (347), p. 1.

McCartney M. 2013. How do we know whether medical apps work? *BMJ 2013*; 346 doi: http://dx.doi.org/10.1136/bmj.f1811

Medscape. 1994 - 2014. "Definition." Retrieved 04 - May - 2014, from http://www.Medscape.com/

Mirza, F., Norris, T., and Stockdale, R. 2008. "Mobile Technologies and the Holistic Management of Chronic Diseases," *Health informatics journal* (14:4), pp. 309-321.

Moyle, E. 2013. "Why Cloud Computing Changes the Game for Hipaa Security," in: *Technewsworld*.

Munro, D. 2013. "Hipaa Support Widens in Cloud Vendor Community," *Forbes [Internet]*).

MyFitnessPal. 2005 - 2014. "Lose Weight with Myfitnesspal." Retrieved 04 - May - 2014, from http://www.myfitnesspal.com/

MyNetDiary Diabetes Inc. 2013. "Mynetdiary Diabetes." Retrieved 22 - May - 2014, from http://www.mynetdiary.com/diabetes-tracker-for-iPhone.html

P A Consulting, G. 2012. "Policy and Regulation for Innovation in Mobile Health." Retrieved 16 - April - 2014, from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/04/policyandregulationforinnovationinmobilehealth.pdf

Piette, J. D., Mendoza-Avelares, M. O., Ganser, M., Mohamed, M., Marinec, N., and Krishnan, S. 2011. "A Preliminary Study of a Cloud-Computing Model for Chronic Illness Self-Care Support in an Underdeveloped Country," *American journal of preventive medicine* (40:6), pp. 629-632.

Remedy Health Media, L. 2014. "Health Mobile Apps Raise Concerns About Safety, Privacy, Health Costs." Retrieved 11 - April - 2014, from http://www.healthcentral.com/diet-exercise/c/255251/162564/apps-concerns-privacy/

Research, J. o. M. I. 2013. "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems." Retrieved 03 - April - 2014, from http://www.jmir.org/2013/8/e186/

Rodrigues J, Diez I, Abajo B. 2012. *Telemedicine and e-health services, policies, and applications: advancements and developments*. Hershey: Medical Information Science Reference.

Rui, Z., and Ling, L. 2010. "Security Models and Requirements for Healthcare Application Clouds," *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268-275.

Schulke, D. F. 2013. "The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing," *Boston University Law Review* (93:5).

Scott, K. M., Gome, G. A., Richards, D., and Caldwell, P. H. 2015. "How Trustworthy Are Apps for Maternal and Child Health?," *Health and Technology* (4:4), pp. 329-336.

Senft, D. J. 2013. "Mobile Devices: Technology Aid--Security Risk," *Geriatric nursing (New York, N.Y.)* (34:2), pp. 149-150.

Supplemental Health Care. 2014. "Health Care on the Go." Retrieved 01 - May - 2014, from http://www.supplementalhealthcare.com/blog/2013/healthcare-go-pros-and-cons-mobile-health-apps

Tamrat, T., and Kachnowski, S. 2012. "Special Delivery: An Analysis of Mhealth in Maternal and Newborn Health Programs and Their Outcomes around the World," *Maternal and child health journal* (16:5), pp. 1092-1101.

Tech-Target. 2009-2014. "Definition: Mhealth." Retrieved 31- March - 2014, from http://searchhealthit.techtarget.com/definition/mHealth>

Technologies, A. 2014. "Mhealth - Its Advantages and Disadvantages." Retrieved 16 - April - 2014, from http://attunelive.com/blog/mhealth-its-advantages-disadvantages/

UCSF. 2012. "Self-Tracking May Become Key Element of Personalized Medicine." Retrieved 01 - May - 2014, from http://www.ucsf.edu/news/2012/10/12913/self-tracking-may-become-key-element-personalized-medicine

Verasoni. 2012. "Mobile Health Applications: 2012 Study ", from http://verasoni.com/2012/08/mobile-health-applications-2012-study/

Vodafone Group. 2013. "Evaluating Mhealth Adoption Barriers: Privacy and Regulation." Retrieved 01 - April - 2014, from http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf

Wang, J., Zhang, Z., Xu, K., Yin, Y., and Guo, P. 2013. "A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System," *International Journal of Security & Its Applications* (7:4).

WebMD LLC. 1994 - 2014. "Public Health in the Smartphone Era." Retrieved 15 - April - 2014, from http://www.medscape.com/viewarticle/776278_3

WellApps. 2009 - 2011. "Well Apps." Retrieved 12 - May - 2014, from http://www.wellapps.com/

Wikipedia. 2014. "Mobile Technology." Retrieved 20 - April - 2014, from http://en.wikipedia.org/wiki/Mobile_technology

An earlier version of this paper was presented at the Australasian Conference on Information Systems (ACIS) 2014 in Auckland, New Zealand.