Investigating Privacy and Security Challenges of mHealth Applications

Research-in-Progress

Stacy Mitchell
University of North Carolina-Wilmington
Mitchells@uncw.edu

Scott Ridley
University of North Carolina-Wilmington
Sr3214@uncw.edu

Christy Tharenos
University of North Carolina-Wilmington
Tharenosc@gmail.com

Upkar Varshney
Georgia State University
Uvarshney@gsu.edu

Ron Vetter
University of North Carolina-Wilmington
Vetterr@uncw.edu

Ulku Yaylacicegi
University of North Carolina-Wilmington
Yaylacicegiu@uncw.edu

ABSTRACT

Privacy and mHealth are fast becoming an important influence on the U.S. healthcare system. The most visible element of mHealth is the profusion of mobile phone applications, especially ones related to wellness. Before researchers can fully examine the impact of mHealth on healthcare, barriers to use need to be addressed. One of the barriers most cited by medical professionals and patients is lack of adequate privacy and security policies and regulation for mHealth apps. In this paper the current state of data security in mobile apps is investigated by conducting a physical forensics analysis of several widely used mHealth applications. We report on the kinds of personal data that can be uncovered both before and after applications are removed and/or secured on a mobile device. These results can be used to develop a set of recommendations that can help to inform users, developers and policy stakeholders of best practices. We also introduce a policy framework for mHealth apps and discuss future work.

Keywords

mHealth, mobile health, forensics, privacy, security, policy, PHR, applications.

INTRODUCTION

Mobile Health (mHealth) is used to denote how mobile and wireless technologies can be used to improve health-related services. The field of mHealth has undergone rapid changes and continues to move up the healthcare agenda (Istepanian et al., 2012; Sebelius, 2011; Varshney, 2011). Fifty percent of the US population now has a smart phone (CTIA, 2011) and these phones continue to develop new features and see improvements in computing power. Smart phones can now be used to track, manage and improve health (Kailas et al., 2010; Landau, 2012a; Landau, 2012b). Perhaps the most visible element of mHealth is the profusion of phone applications (apps), especially the ones related to fitness and wellness. A simple search in application stores shows the presence of a large number of such applications. In addition, market research firms have issued predictions for global health application downloads in 2012 that vary widely from over 40 million to nearly 250 million (PWC, 2012). mHealth "apps" are widely used by consumers and medical professionals (e.g., patients, doctors, pharmacists, and others). A recent report from the Consumer Electronics Association indicates that more than a third of consumers are willing to send medical data to their doctor over a wireless device (Cerrato, 2011). The main categories of mHealth apps that are in use are reference apps (such as WebMD), wellness applications (such as MyFitnessPal), social media apps (such as PatientsLikeMe), and apps designed to access electronic health records (such as Care360) and personal health information (such as Microsoft HealthVault) (mHIMMS, 2012).

In another report, commissioned by Royal Philips Electronics, it is reported that a growing number of mobile users are turning to – and trusting – mHealth applications (RPE, 2012). One in ten Americans surveyed in the study believe that if it were not for web-based health information, "they might already be dead or severely incapacitated". A quarter of those surveyed use symptom checker websites or home-based diagnosis technology as much as they visit the doctor, while another 27 percent use these interactive applications instead of going to the doctor.

Although, there is currently little evidence-based research that can directly support the health benefits of mHealth applications, there is good reason to believe that these applications have potential to significantly benefit overall health. We believe the most benefit potential lies in applications designed to access electronic health records (EHRs) and personal health information (PHIs), however, both patients and doctors need to know that privacy, security, and safety of these applications are adequately addressed before mHealth can be successfully integrated into the healthcare system.

mHealth apps allow patients to take control of their own health, especially in areas of healthy eating, managing chronic disease and quitting smoking (Varshney, 2011). Additionally, personal health records (PHRs), which include medical history, laboratory health results, and insurance information, help people manage their lives and actively participate in their own health care (Pratt et al., 2006). For doctors, mHealth can help provide point of care resources and aid in managing their practices. Patients predict that mHealth will improve the convenience, cost and quality of their healthcare in the next three years (PWC, 2012). mHealth is an important tool in the healthcare arena and its significance and success or failure will be determined from how it integrates with the health systems and allows for better care of patients.

Populations that currently use mobile health technologies have the most to benefit from the use of this technology. The patients with chronic health conditions, as well as people who want to maintain good health would benefit from the implementation of mHealth (Varshney, 2011). As more patients become aware of the health benefits of mHealth, they are anticipated to increase subscriptions to mobile technologies and health applications. According to a Price Waterhouse Cooper (PWC) survey of mHealth, within three years 50-75% of patients expect to use some form of mobile health, primarily information/scheduling and wellness apps (PWC, 2012).

For doctors, mHealth apps can help provide point of care resources and aid in managing their practices. Doctor's list privacy and security as concerns as the leading barriers to greater use of mHealth and only one half of doctors believe that the mobile Internet facilities at their workplace are reasonably secure (PWC, 2012). Patients using mobile health applications need to have confidence that the products they are using are safe, secure and accurate. Data security, access control, policy and confidentiality are the main issues that must be addressed in order for mHealth to continue to flourish and deliver safe healthcare benefits.

Our research is aimed at consumers of mHealth apps. HIMMS classify the mobile applications into two categories: native apps, which reside on a mobile device and require download through a marketplace and non-native apps which utilize browser interfaces (mHIMMS, 2012). Our approach is to use forensic analysis and testing to show that current native mHealth apps lack necessary privacy and security controls. This is especially important for apps that store electronic health records (EHR) or personal health information (PHI) and exchange that data with health-related web sites. We hope that our results can be used to inform and guide policy recommendations, and we suspect that most users are unaware of the potential issues that a forensic analysis reveals about policy, security, and privacy.

The rest of this paper is organized as follows. In the next section, we provide additional background information and discuss the current landscape of mHealth. The development of a policy framework for mHealth apps is introduced next followed by preliminary results from forensic analysis of several mHealth apps. We conclude with a discussion of future work.

CURRENT LANDSCAPE OF mHEALTH

As the United States has moved toward the development of a national Health IT infrastructure, mobile medical applications have been developed to assist both patients and their clinicians in managing care (Merrell et al., 2011). The growing use of these applications, as well as the potential risks that those functioning as medical devices may pose to public health, prompted the United States Food and Drug Administration to issue draft guidance concerning the regulation of mobile medical applications in July 2011 (FDA, 2011).

Several types of mobile medical applications that are proposed to be included in regulations are those that use attachments, display screens, or sensors similar to an existing medical device. However, those medical applications that are intended to be used as devices are a relatively small proportion of those available for use. There are numerous types of applications that are not being considered for regulation. First and foremost, those applications that are used as reference guides for clinicians (Freshwater, 2011; Oehler et al., 2010) and health and wellness records (e.g. diet and weight logs, prescription reminders, etc.) for consumers (Jen, 2010; Kailas et al., 2010) are not being considered for regulation.

Due to the lack of guidelines, laws, and directives applicable to these consumer-based interactive mHealth applications, the burden of consumer protection falls to the application developer. This burden is addressed within the developer license agreement that must be accepted by all creators of applications that deal with mHealth issues. While there are currently more than 20,000 mHealth applications in the marketplace, the number continues to grow across all mobile platforms (Maliszewski, 2012). In order to better understand the current policies that developers are required to adhere to, a review of mHealth application developer license agreements by marketplace was conducted and is summarized in Table 1.

Company	Marketplace	Agreement Policy & Regulation	
		Compliance	Privacy/Security
Apple	iTunes	All national and international regulations, policies, and laws.	Developer responsible for claims arising under consumer protection or similar legislation.
Android	Google Play	None Listed	Developers must protect and the privacy and legal rights of others, and if personal or sensitive information is provided by users, developer must do so securely.
Blackberry	Blackberry World	All applicable privacy legislation.	Developer must use best efforts to ensure confidentiality of end-user data via encryption or similar means.
Windows Phone	Windows Phone Store	All applicable laws and regulations.	Developers collecting or transmitting any user's personal information must alert end-user of this activity.

Table 1. Marketplace Policy for Developers

Regulatory and Security Concerns

mHealth apps may pose considerable security risks to their users and regulations are beginning to be considered by several governmental and business groups. Table 2 shows the list of federal agencies governing the mHealth landscape in the U.S. These agencies are the Federal Communications Commission, the Food and Drug Administration, the Federal Trade Commission, the Office for Civil Rights, and the National Institute of Standards and Technology (Roney, 2012).

The Agency	The Role
Food and Drug Administration (FDA)	regulates products including software, hardware, or devices combining them
Federal Communications Commission (FCC)	The FCC authorizes a wide variety of RF-based medical devices including both implanted devices (e.g., heart pacemakers) and patient monitoring devices (e.g., wireless telemetry). It also authorizes carriers whose networks are used by a wide variety of mobile devices (e.g., smartphones) to access, store or transmit health information, and it establishes technical rules used by WiFi and other similar networks.
Federal Trade Commission (FTC)	regulates interstate commerce and works for consumer protections including mobile data security
Office of the National Coordinator for Health IT (ONC)	provides guidance and support for the nation's health IT infrastructure
Department of Health and Human Services' Office for Civil Rights	responsible for implementing and enforcing the HIPAA
National Institute of Standards and Technology (NIST)	The Computer Security Division, one of six divisions within NIST's Information Technology Laboratory, is responsible for developing standards, guidelines, tests and metrics for the protection of non-national security Federal information and information systems.

Table 2. Federal Agencies Regulating and Governing the mHealth in the US

mHealth applications may contain sensitive patient information, such as past and current medical conditions, diagnostics, prescriptions and lab results, along with the identifying information patients give when they create their profiles. Most of the time, it is not clear to the users if the sensitive information is shared by the third parties, how it is stored, whether it is stored with any identifying data or whether the app is "mediated by a human being or not" (Cerrato, 2011).

In addition, concerns over an app's clinical appropriateness and technical functionality have led one healthcare-focused app store, Happtique, to announce plans to certify mobile health apps (Dolan, 2012). Because of the large number and wide variety of mHealth apps already available, it will be some time before the certification of apps is completed. Recent estimates of the number of health-related apps for both consumers and medical professionals in Apple's AppStore alone top 20,000 (Dolan, 2012).

Regulatory Compliance for Health, Medical and Related Apps are also addressed in app store license agreements for developers. For example, the Apple iOS Developer Program License Agreement (section 3.3.26) states that all submitted applications to Apple selected for distribution must "represent and warrant" that the developer is in full compliance with all applicable laws, regulations, and policies (in particular the U.S. Food and Drug Administration). Further, developers must comply with all laws, regulations and policies of any other applicable regulatory bodies in any country or territory where their applications are used or made available.

Role of App Stores

It is critical that developers be aware of app store policies regarding health-related applications prior to submission to a store and ultimately user download. Many apps use a backend service, such as Microsoft Health Vault, to store the user's data in the cloud. Additionally, we have found that app data and/or pointers can be located in at least six locations on the mobile device highlighting either an inefficient operating system (OS) or a poorly written mHealth app.

There are currently four major app marketplaces. Which marketplace the user chooses is determined by the mobile device OS (iOS, Android, Windows Phone, Blackberry) and to a lesser extent the OS version installed.

- Apple's marketplace, iTunes, currently lists over two-hundred-and-forty medical apps. An example such as Medscape has over twenty-thousand ratings to date.
- Google Play, the Android marketplace, lists approximately four-hundred-and-eighty apps after using "mHealth" in a keyword search. WebMD is the resultant top app with over eleven thousand ratings at this time.
- Windows Phone Store has very limited search and navigation functions making it difficult to present, close to, accurate numbers. Searches using the keywords "emr" and "medical" did not return useful information. A side-bar navigation to "health" resulted in approximately four-hundred-and-forty apps. These results combine mHealth, personal health, personal fitness, medical and "other medical." The top app is currently unavailable.
- Blackberry World is the most limited app store in terms of general mHealth applications but offers the most institutional specific mHealth apps in one marketplace. A keyword search using the term "medical" return over two-hundred-and-five apps. Research in Motion (RIM), currently doing business as Blackberry, is known to offer devices with high encryption and secure mail and messaging services. Certain governments have requested RIM to provide encryption keys or place communication servers within their respective country to facilitate government monitoring of communications.

The summary of our search is shown in Table 3. This includes 4 major app marketplaces along with the number of mHealth Apps, top rated mHealth Apps and ratings. Additional explanation is provided below the Table**.**

App Marketplace	Productive Keyword Search	No. of mHealth Apps	Top Rated mHealth App	No. of Ratings for Top mHealth App	Notes
iTunes	emr, medical, mhealth	240	Medscape	20,000+	1, 2
Google Play	mhealth	480	WebMD	11,000+	1, 2, 3
Windows Phone Store	none	440	NA	NA	1, 2, 4, 5
Blackberry World	medical	205	NA	NA	1, 2, 5

Notes:
(1) Keyword search returned some apps that would provide little use to end-users. Some apps may be medical references as well.
(2) Number of mHealth related apps is an approximation based on data from the respective manufacturer's website
(3) Top rated app is current at the time of this writing with number of ratings rounded to nearest thousand
(4) All mHealth and medical apps collectively placed with general health apps
(5) Unable to determine top-rated app due to marketplace layout

Table 3. The Summary of Our Search

POLICY FRAMEWORK FOR mHEALTH APPS

mHealth devices come under the regulatory authority of the Food and Drug Administration (FDA) in the United States. In mHealth FDA regulates products including software, hardware, or devices combining them. The importance of the concept of medical use is the intent of the person who develops/sells it that gives it a medical use quality. FDA considers the words, actions, and recommendations to customers as the method for determining intended use. With products such as artificial heart valves, the intent of medical use is clear; however, for a product such as a hardware/software aiding sleep, FDA could label it as a wellness device unless it is marketed as a treatment for a sleep disorder, which makes the product a medical one. If a product is labeled as a medical product, then it will be subject to regulation by the FDA and must be tested and evaluated using their standards.

We have developed a policy framework which includes the following guidelines to improve the privacy and security for mobile health applications.

- CONTEXT: Provide details about the applications, its capabilities and limitations, and its use of patient information.
- MINIMIZATION: Minimize the amount of information that is collected from/about the patient.
- INFORMED CONSENT/AWARE-PATIENT: The patient should be made aware of how the information will be used and has been used by the application. What information is needed for providing certain healthcare benefit could also be stated to the patient. A more aware patient is likely to make better decisions about tradeoffs involving information privacy-security and healthcare benefits.
- OWNERSHIP: The ownership of the information should be well defined meaning who owns the user data even in anonymous form.
- DELETION-AFTER-DEACTIVATION: If a patient has deactivated an application, all information about/from the patient should be deleted.
- SECURE STORAGE: The information should be kept securely at device, server or cloud. To reduce transmission over wireless networks, information that is subject to change can be stored locally, while more static information can be kept at a server.
- END-TO-END: Various weak points in the end-to-end security should be identified and efforts be made to correct these weakness in applications, devices, operating systems, networks, servers, among others.

These guidelines can be used to develop more specific guidelines for applications developers, service providers and patients. Based on the potential use/abuse of patient information due to either or combination of security and privacy weaknesses, the patients have to decide (a) what information should be provided to m-health applications and when, (b) what are the tradeoffs of privacy and healthcare benefits (meaning how an increased level of privacy could affect some of the benefits), and (c) how the current condition/level of emergency may affect what information can be used and how.

The proposed framework should result in several health benefits including increased user confidence in mHealth applications, the minimization of adverse healthcare effects, and the adoption of best practices for healthcare. We also expect broader impacts on legal/regulatory policies for mHealth on regional and state levels.

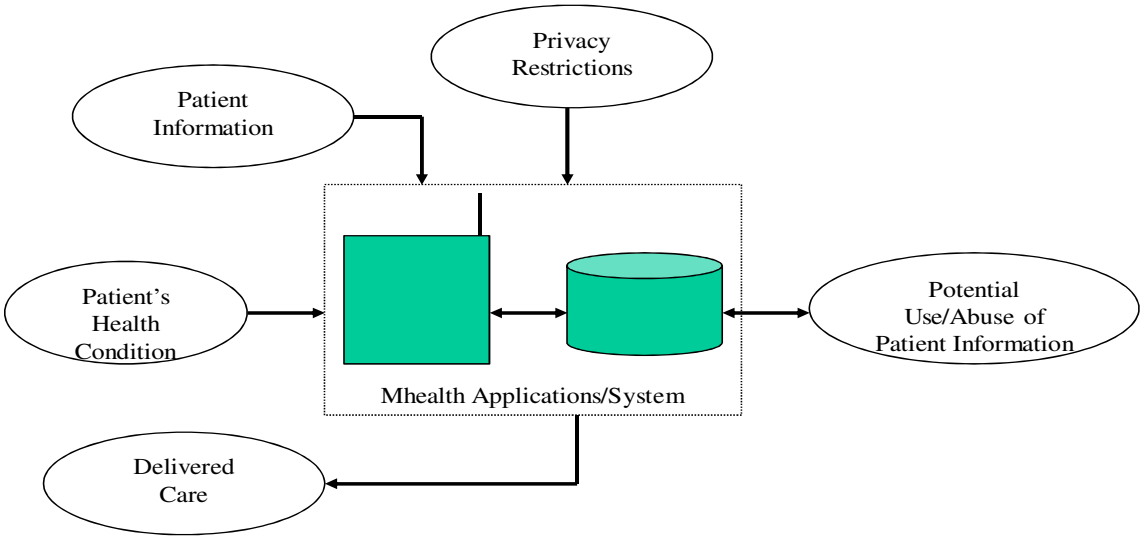


Figure 1. The Model used in the Policy Framework

FORENSIC ANALYSIS AND ASSESSMENT

Mobile Device Forensics

Mobile device forensics (mobile forensics) is a branch of digital forensics that is primarily focused with the recovery of digital data on a mobile device. A mobile device can be classified as a GPS device, dumb-phone, feature-phone, smartphone, MP3 player or tablet, such as the Apple iPad or Microsoft Surface RT. Mobile forensics is a growing field due to the number of devices currently owned across the globe, the number of devices being brought to market on a quarterly basis and manufacturers looking to streamline future operating systems. As mobile devices have become "smarter" they have also become more personal, allowing users to access and store a plethora of data at their fingertips. Every mobile operating system (OS) platform has its own application (app) store allowing users to further personalize their mobile device.

There are several mobile forensic tools available today. These can range from free database viewer software to forensic extraction devices with hundreds of device cables. A few of the most prominent manufacturers in the mobile forensics field are Katana, Cellebrite and Micro Systemation.

By capturing data below the logical layer, more in depth than a logical extraction but not a true physical extraction, of a mobile device we have been able to determine that the user data collected by apps can be accessed quite easily as security standards are not yet fully implemented by device makers, OS manufacturers, app programmers or the various levels of government. The data that can be discovered from a mobile device includes call history, sent and received Short Message Service (SMS) and multimedia messages, contacts and phone numbers, emails, photos, videos, geo-location and GPS information, wireless network settings, Web browsing history, voicemail messages, social networking information, application histories and logs, and other data that might be retained within smart phone apps.

The procedure developed and used in our mobile forensic lab to test the validity of an app and to image a smart phone is a multi-step process. First, the appropriate mobile device is selected, cleared of all data and reset to factory defaults. If activation is required the device is activated followed by the installation of the apps being researched. Prior to accessing any of the apps the mobile device's data is extracted using two forensic tools (referred to as "pulls"). Once the pulls have been examined the apps can now be populated with user data. At the completion of data population the mobile device is put through another set of pulls that are then checked for corruption. At this point all apps are removed from the mobile device by manually deleting the app as a user would. Another set of pulls are performed on the mobile device and are checked for corruption. The mobile device is now cleared of all data, reset to factory settings, and placed through a final set of pulls.

From here the pulls are collectively investigated using much smaller forensic tools such as database and plist viewers. At the conclusion a working report is compiled and submitted for review.

Forensic Analysis

In our research lab we have several products that can perform both logical and physical pulls. Our current work involves performing forensic analyses of several mHealth apps both before and after they were installed, secured, and then removed from the device. Initial results have found that many apps store unencrypted personal information on the mobile device itself. For example, log files from a top-downloaded app showed clear-text instead of encrypted text when an error occurred during transmission. The two examples below highlight the kinds of data that can be uncovered during a forensic analysis.

Figure 2 shows personal health related diseases entered into a mHealth app by an end-user that has been forensically recovered. Note that the insurance carrier and several diseases are readily apparent in the data.

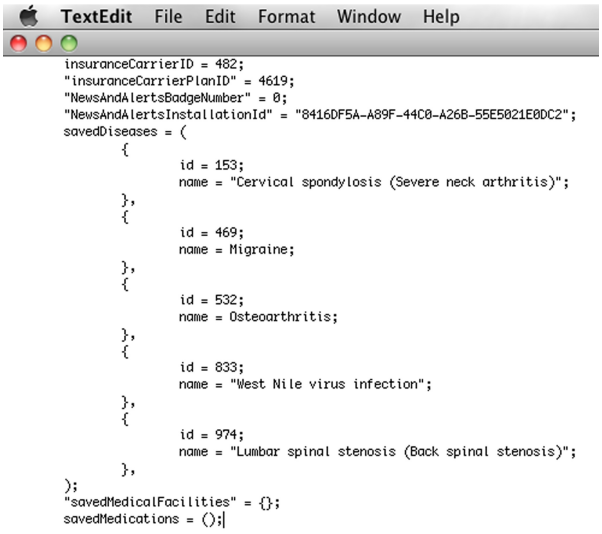
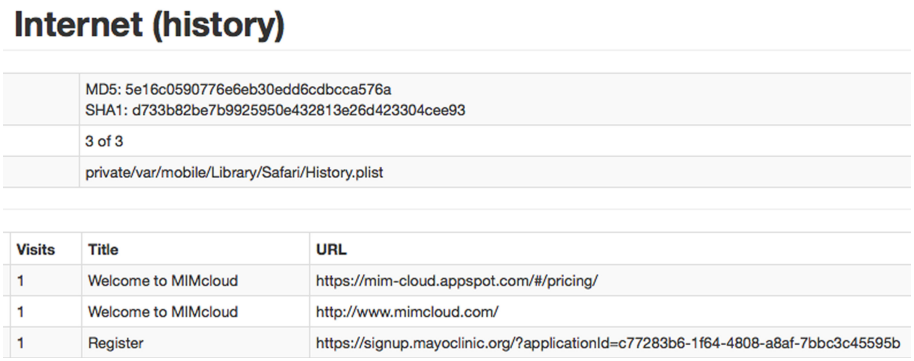


Figure 2. A Sample Capture

Figure 3 below identifies internet activity, web addresses, the directing app product identification number (where applicable) and the number of visits. This information may be used to identify which medical web sites were visited by the user as well as likely search topics of interest.



Internet (history)

	MD5: 5e16c0590776e6eb30edd6cdbcca576a SHA1: d733b82be7b9925950e432813e26d423304cee93
	3 of 3
	private/var/mobile/Library/Safari/History.plist

Visits	Title	URL
1	Welcome to MIMcloud	https://mim-cloud.appspot.com/#/pricing/
1	Welcome to MIMcloud	http://www.mimcloud.com/
1	Register	https://signup.mayoclinic.org/?applicationId=c77283b6-1f64-4808-a8af-7bbc3c45595b

Figure 3. A Sample Capture of Internet History

DISCUSSION

During our forensic analyses we found that many apps stored unencrypted personal information on the mobile device. Our research, through the use of mobile device forensics, has also found that many applications (apps) store unencrypted personal information on the mobile device itself. The log files from a top-downloaded app show clear-text instead of encrypted text when an error occurred during transmission.

The unencrypted information stored on mobile devices by mHealth apps include, but are not limited to, the users' name, birth date, country, culture preference(s), preferred language(s), personal app identifier, insurance carrier identifier, medical conditions, medications, physician(s), and pharmacies. These data examples do not include physician mHealth apps that may contain anything from patient records to medical images. Not only is app and network security a great concern, physical security poses a large risk, such as the loss of a mobile device.

Without app marketplaces policing and monitoring mHealth app submissions and current inventories, we expect that we will continue to see unencrypted personal medical information in our forensic analysis examinations. Oftentimes, OS manufacturers hide details concerning data security and data collection policies within the tens of pages of legalese offered to end-users and end-users simply click "Agree."

CONCLUSIONS AND FUTURE WORK

Through literature review and forensic analysis, we found a broad range of new information that aided us in developing policy recommendations for mHealth applications, including: data on barriers to mHealth usage, such as concerns about privacy and security, how a lack of policy and regulation influences healthcare compliance and best practices, and the lack of user knowledge about mHealth privacy and security.

The findings in this paper will result in several health benefits including increased user confidence in mHealth applications, the minimization of adverse healthcare effects, and the adoption of best practices for healthcare. We also expect broader impacts on legal/regulatory policies for mHealth on regional and state levels with further research.

Future work includes (a) the development of a white paper that can be submitted to various government agencies at local, state and federal levels including FDA which are interested in guidelines for mobile health applications, (b) the submission of recommendations to device and equipment manufacturers and mobile applications developers to further improve their offerings, and (c) the development of patient education material that addresses key points in using mHealth applications regarding security, safety and privacy.

REFERENCES

1. Cerrato, P. (2011) Mobile medical apps meet the FDA, Part 2, *Information Week* (available http://www.informationweek.com/healthcare/mobile-wireless/mobile-medical-apps-meet-the-fda-part-2/231901916).
2. CTIA (2011) Nationwide Wireless Quick Facts, (available http://www.ctia.org/advocacy/research/index.cfm/aid/10323).
3. Dolan, B. (2012) Mobihealthnews, (available http://mobihealthnews.com/15750/happtique-steps-up-to-certify-mobile-health-apps).
4. FDA (2011) Draft guidance for industry and Food and Drug Administration staff - Mobile medical applications, (available http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm263280.htm).
5. Freshwater, M. (2011) iPhone and iPad applications for plastic surgeons, *Journal of Plastic Reconstructive Aesthetic Surgery*, 64, 1397-1399.
6. Istepanian, R. and Xhang, Y.-T. (2012) Guest editorial introduction to the special section: 4G health - the long-term evolution of m-health, *IEEE Trans on IT in BioMedicine*, 16, 1, 1-5.
7. Jen, W. (2010) The adoption of mobile weight management services in a virtual community: The perspective of college students, *Telemed J E Health*, 16, 490-497.
8. Kailas, A., Chong, C.-C., and Watanabe, F. (2010a) From mobile phones to personal wellness dashboards, *IEEE Pulse*, 1, 1, 57-63.
9. Landau, E. (2012a) Smartphone apps become 'surrogate therapists', (available http://www.cnn.com/2012/09/27/health/mental-health-apps).
10. Landau, E. (2012b) Tracking your body with technology, (available http://www.cnn.com/2012/09/21/health/quantified-self-data/index.html).
11. Maliszewski, S. C. (2012) Certifying mobile health apps: Just what the doctor ordered, (available http://www.mhimss.org/news/certifying-mobile-health-apps-just-what-doctor-ordered).
12. Merrell, R. and Doarn, C. (2011). Medical applications, mobility, and regulations, *Telemed J E Health*, 17, 235-236.
13. mHIMMS (2012) Selecting a mobile app: Evaluating the usability of medical applications, (available http://www.mhimss.org/sites/default/files/resource-media/pdf/HIMSSguidetoappusabilityv1mHIMSS.pdf).
14. Oehler, R., Smith, K., and Toney, J. (2010) Infectious diseases resources for the iphone, *Clinical Infectious Disease*, 50, 1268-1274.
15. Pratt, W., Unruh, K., Civan, A., et al. (2006) Personal health information management, *Communications of the ACM*, 49, 1, 51-55.
16. PWC (2012) Survey of m-health: Emerging m-health-Paths for growth, (available http://www.pwc.com/mhealth).
17. Roney, K. (2012) Becker's Hospital Review, (available http://www.beckershospitalreview.com/healthcare-information-technology/5-important-federal-agencies-for-mobile-health-regulation.html).
18. RPE (2012) Philips survey reveals one in 10 Americans believe online health information saved their life, (available http://www.newscenter.philips.com/us_en/standard/news/press/2012/20121212_Philips_Survey_Health_Info_Tech.wpd#.UZVUN7Xrz7Q).
19. Sebelius, K. (2011) Keynote Address at mHealth Summit, Washington, DC (available http://www.hhs.gov/secretary/about/speeches/sp20111205.html).
20. Varshney, U. (2011) Pervasive healthcare computing: EMR/EHR, wireless and health monitoring, Springer, New York.