Privacy, Security and Interoperability of Mobile Health Applications

Josette F. Jones, Sara A. Hook, Seong C. Park, and LaSha M. Scott

Indiana University School of Informatics, IUPUI
535 W. Michigan Street
Indianapolis, Indiana 46202, U.S.A.
{jofjones,sahook}@iupui.edu

Abstract. This paper will discuss the security, privacy and interoperability of mobile health applications (MHAs) and how these issues must be reconciled in order for MHA devices to be implemented in the most robust fashion. Balance is needed between privacy and accessibility, between security and interoperability and between flexibility and standardization. The interoperability of diverse MHA devices must be a goal for the future in order to realize portability, true continuity and quality of care across a wide spectrum of health services. A pilot project to determine potential threats to the privacy of personal health information on an iPad will be described

Keywords: Security, interoperability, privacy, mobile health devices, usability.

1 Introduction

This paper will discuss the security, privacy and interoperability of mobile health applications (MHAs) and how these issues must be reconciled in order for MHA devices to be implemented in the most robust fashion. Balance is needed between privacy and accessibility, between security and interoperability and between flexibility and standardization. The interoperability of diverse MHA devices must be a goal for the future in order to realize portability, true continuity and quality of care across a wide spectrum of health services. Without some assurance that there will be interoperability, consumers, particularly parents with children or people in other vulnerable populations, will be reticent to invest the time necessary to obtain and fully utilize MHA devices and there will be wide variation in the quality and granularity of information that is collected, displayed and transmitted from these devices. Without privacy and security across state lines and international borders, it is doubtful that children, their parents or their health care providers will trust MHA devices. To better frame the issues, the paper will focus on opportunities and challenges for using MHA devices to address childhood obesity from a legal and health care perspective.

Health care providers and industry experts believe that empowering patients by providing access to their medical information and appropriate resources and tools to manage their health can significantly improve outcomes and reduce costs. The

C. Stephanidis (Ed.): Universal Access in HCI, Part III, HCII 2011, LNCS 6767, pp. 46–55, 2011.

combination of standard health record-keeping function of traditional EHRs and PHRs and action-oriented feedback through MHA devices can enable users to maintain their health and prevent diseases such as childhood obesity. Programs directed towards overweight children and teenagers may contain a number of elements, including a complete medical evaluation, nutritional counseling, home visits, behavioral therapy and fitness skills. In order to be most effective, a social component or "buddy" may also be helpful for providing peer encouragement and peer pressure. Issues remain with respect to the interoperability of MHA devices and the privacy and security of these devices.

2 Literature Review

Recent literature reveals proposed or current uses of mobile and handheld devices for a number of different health care applications, particularly for the physician and other health care professionals. For example, Bellamy et al. report that the Osteoarthritis Index can be delivered by mobile phone in a way that is valid, reliable and responsive[1]. Other authors propose changing the paradigm of mobile phones to something they refer to as a personal wellness dashboard [2, 3]. However, the need for regulations, standards, industry alliances, security, reliability and minimal discomfort in data collection is needed. Among the user centric applications proposed for Smartphones are personal health records (PHRs), medication adherence and selection programs, physician selection and second opinions, monitoring physical well-being, including fitness and diet, health and disease monitoring and management, including home monitoring, and healthy lifestyle suggestions. Patrick et al. discuss some policy issues for mobile phones, including usability and access, data security and interface with personal and medical health records [4].

Health and Hospital Networks (H&HN) (September 2010) reported that at Vanderbilt University Medical Center anesthesiologists are allowed to check vital signs, communicate with colleagues and observe operating rooms from their cell phones. Remote health monitoring using mobile phones [5] and the next generation of telehealth tools for patients [6] also present some potentially powerful opportunities for mobile health applications devices. Likewise, Blake reports on the use of mobile phone technology in chronic disease management, including monitoring health status, electronic tracking, patient self-management and improving health communication [7].

What is perhaps the more interesting aspect of mobile health devices is when they are operated and controlled by patients. Krishna and Boren provided a systematic review of self-management care via cell phone for diabetes patients [8]. Bernabe-Ortiz et al. reported on a comparative study in Peru involving the use of handheld computers for collecting sensitive data from citizens in surveys as compared with paper-based surveys [9]. The study indicated that it was feasible to develop a low-cost application for handheld computers that could collect data on sexual behavior and that this was a viable alternative to paper forms. However, the concerns with the privacy and security of personal health information, especially when collected, stored and transmitted using a mobile device has not been fully explored. Moreover, there may

be additional concerns when the patients who are using these devices are children, most of whom do not have the authority to provide consent for or make decisions about their own medical care.

Shieh et al. note a number of challenges with mobile healthcare, including the need for interoperability among electronic health records, developing better display technologies and security controls and developing smart algorithms to detect clinically significant events before notifying caregivers [10]. Likewise, Pharow and Blobel asserted that aspects of security, safety, privacy, ethics and quality reach importance when discussion health information and health systems, including mobile solutions and that there are both legal and technological challenges [11].

3 Challenges of the Use of MHA

3.1 Interoperability

Interoperability in the context of health information technology is traditionally viewed in terms of connectivity: Information can be exchanged over a common medium in a secure, accurate and efficient way without special effort on the part of the user. To address the epidemic of childhood obesity and related issues, interoperability has to surmount not only the connectivity for health information exchange- local to global- the medical efforts must be coupled with observational data from the daily environment outside the clinic walls. Interventions to address childhood obesity combine data from disparate sources (i.e., combining provider data from multiple EMRs, payers, labs, dental services, nutritional services, school nurses, childhood obesity registries, parents or guardians), record matching services are needed [12]. Any MHA therefore will need interfaces to external applications to retrieve child data located across disparate ancillary systems; requesting attention to syntactic interoperability – structure to the information – and semantic interoperability – Information is understood by everyone involved in the care of the individual [13]. The National Broadband Plan (2010) and the push to adopt health IT support these priorities by dramatically improving the collection, presentation and exchange of health care information, and by providing clinicians and consumers the tools such as MHA to transform care. Technology alone cannot heal, but when appropriately incorporated into care, technology can help health care professionals and consumers make better decisions, become more efficient, engage in innovation, and understand both individual and public health more effectively.

3.2 Privacy

Most U.S. citizens may be under the impression that privacy is a right accorded them through the U.S. Constitution. In one sense, this is true, in that a number of the Amendments do have an underlying theme of privacy, including the right to free speech and association, freedom of religion and freedom from unreasonable search and seizure. On the other hand, privacy has also evolved through a number of famous cases, including *Roe v. Wade*, *Griswold v. Connecticut* and *Loving v. Virginia*.

A patchwork quilt of statutes at the federal level have attempted to address privacy issues related to various specific facets of modern life, including the Gramm-Leach-Bliley Act for financial information and the Health Insurance Portability and Accountability Act (HIPAA) for personal health information. The tension between national security and privacy is a more recent concern, given the enactment of the U.S.A Patriot Act and the seemingly more generous allowance for law enforcement to use technology for surveillance without a warrant. Indeed, privacy may be the "civil rights" issue of the next decade. Likewise, states also grapple with privacy from a number of vantage points, including statutes for health records, for public records and for information related to children.

At the same time, there seems to be a lack of concern for privacy on the part of some people, particularly children and adolescents. The desire to participate in social networking sites such as Facebook, YouTube and MySpace may mean that young people are revealing personal information that not only puts them at risk from child predators, but may also cause harm later. It is now not uncommon for information posted on these social networking sites to be used by schools for disciplinary purposes, by future employers, by law enforcement and by attorneys. It is also unclear how companies who are providing "hosting" services might use the information now or later. Abril and Cava note that "[m]any privacy breaches on social media occur at the mouse-clicks of fellow cyber-patients or are facilitated by the patients themselves…As evidenced by numerous surveys, the majority of website users do not understand, access or know the significance of privacy policies and terms of use" [14].

In articulating a research agenda for PHRs, Kaelber et. al note that "[p]atient's greatest concern about nearly every type of electronic healthcare applications, including PHRs, is security and privacy. Ninety-one percent of people report they are 'very concerned' about the privacy and security of their personal health information" [15]. This article also notes several important issues regarding PHR privacy – who controls sharing and acing of the information in the PHR, how to optimally design PHR systems in order to allow patients to maximize the security of their PHRs and who to develop authentication methods that ensure both privacy and security yet do not present a major barrier to access [15]. As the article states, "[c]lear tradeoffs exist between privacy, security and access, even for patients [15]. Clearly, the issues are even more complex with any device or system that gathers personal health information from children, especially when trying to design a MHA device tailored for children with obesity.

In terms of protecting patient privacy in the information age, Kendall notes that "[t]he loss of privacy seems to be a foregone conclusion in the information age. Polls show that most Americans believe they have lost all control over the use of personal information by companies. Americans are also concerned about the threats posed by identity theft and fraudulent internet deceptions like phishing. People are learning the hard way to withhold information unless it is absolutely necessary to disclose it" [16]. A reluctance to provide personal health and financial information is not difficult to understand, given the many high-profile reports of data security breaches from some

top companies and organizations. These breaches are not just caused by a lapse in computer security practices, but have often occurred because of stolen laptops and misplaced back-up tapes. With identity theft that fastest growing crime in American, followed closely by Medicare fraud, the heightened awareness about data security on the part of the public is not surprising. For example, many people are now taking advantage of laws in various states that allow them to "freeze' access to their credit reports. Therefore, any MHA device must be able to ensure the privacy of its information, especially the personal health information of children, while still being appealing, accessible and easy to use.

3.3 Security

It is fair to say that the public is keenly aware of the security risks to computer systems and networks, particularly when breaches in security may mean that their personal health and financial information is vulnerable. Indeed, identity theft is the fastest growing crime in the U.S., followed closely by Medicare fraud; both of these crimes are greatly facilitated by technology, particularly where the individual consumer or patient has little control and can only take remedial action once a breach has occurred. For example, in a report dated February 10, 2010, more than 500,000 current and former members of BlueCross BlueShield of Tennessee will be receiving letters altering them that their personal information was included on computer hard drives stolen from the insurance company last year [17]. Another aspect of security that many people fail to consider is disaster planning. Natural disasters, such as earthquakes and floods, as well as manmade disasters like broad attacks on an individual company or network or on the nation's Internet infrastructure, may also impact the security of mobile health devices and the systems that run them. Individual MHA devices may be particularly at risk, being small and easy to steal or lose. Also, since these are wireless devices, there is increased risk that personal health information could be compromised. On the other hand, the trend is for increased virtualization of computer systems to third-party vendors, known as cloud computing. Not only does this pose additional security risks, but this adds another layer of questions on the extent to which personal health information is protected.

Mobile health application devices, which have the advantages of portability and accessibility, can also present security threats, as reported by Wright and Sittig [18]. Fortunately, these devices also can also be equipped with encryption and security features, such as passwords, and are designed to be attached to a keychain or lanyard and carried with the patient [19]. At the time of their study, many manufacturers of USB-based personal health records were still in the development phase for their products. Of course, in terms of pediatric mobile health devices, a significant issue will be keeping track of the device itself rather than just protecting the information on the device, given the propensity of young people losing things. On the other hand, the transition from desktop and laptop computers to smaller mobile devices means that both physical and information security for these devices must be considered if they are to be useful on a regular basis for children with obesity. For example, a mobile health device for children with obesity might be designed to allow for regular input of

food consumption, either via text, pre-programmed pull-down menus or camera phones and the logging of physical activity, such as participation in fitness programs, 5K runs/walks and weight lifting.

Another issue with an MHA device for children with obesity is the extent to which the information can be altered. In the context of health information provided in through a PHR, Simborg argues that while there is no question that patients own their PHRs, at least those that are "untethered" from a provider, employer or payor, "advocating the right of a consumer to alter professionally sourced information may put the entire future of PHRs at risk" [20]. This issue is even more complex with a mobile health device for children with obesity, because there would be an additional question of the extent to which a parent or guardian would be allowed to alter information, particularly information that might present the child or the parent in a bad light. On the other hand, health care providers must certainly be concerned with future liability if confronted with health care information contained in a PHR had been altered in a way that suggested unaddressed medical needs.

4 Exploratory Study: Use of the iPad in Health Care

After the iPad was introduced, user comments suggest improved usability and use compared to the previous small screen mobile devices. Increased screen size and better readability of the screens make the iPad more suitable for clinical use. The question though arises if the increased screen size is a threat to privacy and confidentiality of protected health information (PHI).

Upon exploration of the technical specifications, testing some of different types of PDA, and reviewing the literature [21, 22] the following usability, privacy and confidentiality issues have been identified:

- small screen size allows only for display of limited information
- small font size and limited back light
- most WWW sites are poorly formatted for PDA viewing
- patient confidentiality during use of PDA is an area of significant concern and potential problem and is more apparent when larger screen size
- potential for lost or misplacement
- disclosure of PHI
- potential for medical identity theft

Despite these issues, the PDA has been integrated in clinical practice. Usability studies [23] of the recently introduced iPad has proven to be more appealing because of a bigger screen, better visual acuity, easier web browsing, etc. While small screen size and visual acuity may have protected information displayed, the benefits of the iPad may be a drawback regarding privacy and security.

4.1 Methodology

A pilot study was conducted in order to test the privacy of an iPad application. The purpose of this study is to explore (1) the circumstances under which information

posted on the iPad can be seen by bystanders and (2) how well the information can be recognized.

Eighteen visitors at the campus student center were randomly asked if they wished to participate in an iPad confidentiality survey and the purpose of the study and expectations were explained. Participants were assured that no personal information would be asked and that the survey would take only about 5 minutes of their time. Three different scenarios were used for the survey. Each scenario was either in landscape or portrait display of the iPad for the entire survey. Each participant participated in only one scenario and only one display type. The survey scenarios included:

- A mock-electronic health record (EHR) of a patient who is HIV-positive (scenario A)
- A picture of a multi-trauma patient (scenario B)
- A combination of a picture and EHR of a patient (scenario C)

One research assistant asked the participants if they could see the iPad screen from different distances and angles. The distances varied from10 feet, 5 feet and 3 feet away from the iPad, the angles ranged from 180 degrees to 45 degrees. The participant will be sitting or standing behind, in front or next to the research assistant holding iPad. If they can, they will be asked to describe what they can see. These distances were chosen because it is a reasonable distance a patient or companion may be from a physician while they are using the IPad. The description of the display by the participant describes is recorded by research assistant 2. Research assistant 1 will record accuracy of the participant's description.

4.2 Study Results

The results of the study are reported in table 1

As can be deduced from the study results and illustrated in Figure 1, the bystander was able to read and describe the content of the display (codes 1 and 2) in 78.5% of the time. In about 59% of the time, the content was reported correctly; in 21.5% of the time the bystander was unable to see the content of the display.

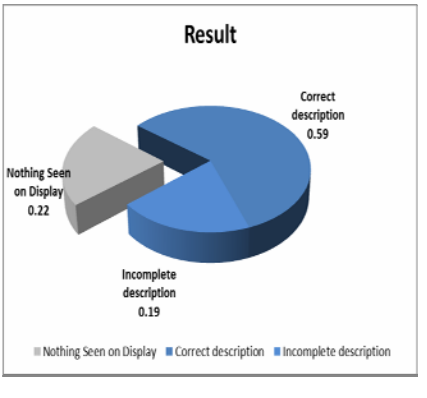
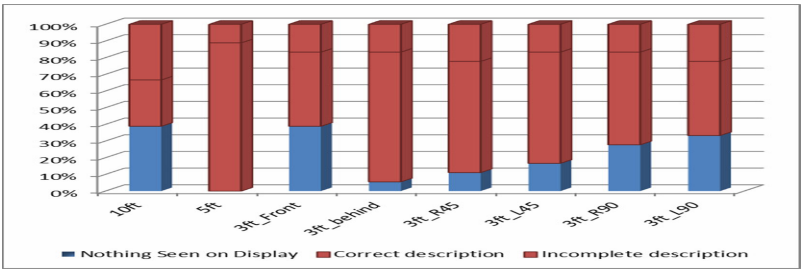


Table 1. Participants report of IPad display

Participant	Scenario	Position 1=standing 2=sitting	Orientation L=Landscape P=Portrait	10 feet	5 feet	3 feet front	3 feet behind	3 feet 45 degrees right	3 feet 45 degrees left	3 feet 90 degrees right	3 feet 90 degrees left
1	B	1	L	0	1	0	1	0	1	0	0
2	B	1	L	0	1	0	1	1	1	1	0
3	C	1	L	0	1	1	1	2	1	0	2
4	C	1	L	2	1	1	1	2	1	1	1
5	A	1	P	0	1	0	1	1	0	0	0
6	A	1	P	1	1	1	1	1	1	0	0
7	B	1	P	0	1	1	1	1	1	1	0
8	B	1	P	1	1	1	1	1	1	1	1
9	C	1	P	2	2	0	1	1	0	2	2
10	C	1	P	2	1	0	1	1	2	0	0
11	B	2	L	0	1	1	1	1	1	1	1
12	C	2	L	1	1	2	2	2	2	2	2
13	A	2	P	0	1	1	0	1	1	1	1
14	A	2	P	2	1	0	1	1	1	1	1
15	B	2	P	1	1	0	1	1	1	1	1
16	B	2	P	1	1	1	1	0	0	1	1
17	C	2	P	2	2	2	2	2	2	2	2
18	C	2	P	2	1	2	2	1	1	1	1

Results coding: 0 = nothing seen on display; 1=correct description of content on display; 2= incomplete description of content on display.

Noteworthy is that from a distance of 5 feet independent of the position, all bystanders were able to describe the content, all or some, of the display. Content on the display is also easily viewed from a distance of 3 feet, the bystander behind the user (see Figure 2).



Health care providers and consumers are likely to use the iPad in the future for medically related tasks, including receiving and reviewing information updates, as a tool during their standard practice and to complete paperwork. Yet the results of this limited study recommend some caution to secure the privacy and confidentiality of PHI.

5 Conclusions

Interoperability, security and safety are on top of the priority list and supersede usability when it comes to protecting PHI. The paper addresses the identification of some specific aspects like mobile technology and safety when moving both IT and people towards mobile health aiming at increasing providers and patients' awareness, confidence, and acceptance in MHA to manage their health.

Acknowledgments. The authors thank N. Blount and B. Pape for their help in data collection. The study is supported by the Bridges to Baccalaureate Program, Indiana University, Indianapolis.

References

1. Bellamy, N., et al.: Osteoarthritis Index delivered by mobile phone (m-WOMAC) is valid, reliable, and responsive. Journal of Clinical Epidemiology 64, 182–190 (2011)
2. Terry, M.: The Personal Health Dashboard: Consumer Electronics Is Growing in the Health and Wellness Market. Telemedicine and e-Health 15, 642–645 (2009)
3. Krishna, S., et al.: Healthcare via Cell Phones: A Systematic Review. Telemedicine and e-Health 15, 231–240 (2009)
4. Patrick, K., et al.: Health and the Mobile Phone. American Journal of Preventive Medicine 35, 177–181 (2008)
5. Agarwal, S., Lau, C.T.: Remote Health Monitoring Using Mobile Phones and Web Services. Telemedicine and e-Health 16, 603–607 (2010)

6. Ackerman, M.J., et al.: Developing Next-Generation Telehealth Tools and Technologies: Patients, Systems, and Data Perspectives. Telemedicine and e-Health 16, 93–95 (2009)
7. Blake, H.: Innovation in practice: mobile phone technology in patient care. British Journal of Community Nursing 13, 160 (2008)
8. Krishna, S., Boren, S.A.: Diabetes Self-Management Care via Cell Phone: A Systematic Review. J. Diabetes Sci. Technol. 2, 509–517 (2008)
9. Bernabe-Ortiz, A., et al.: Handheld computers for self-administered sensitive data collection: A comparative study in Peru. BMC Medical Informatics and Decision Making 8, 11 (2008)
10. Sheih, Y.Y., et al.: Mobile Healthcare: The Opportunities and Challenges. Int. J. Elect. Healthcare 4, 208–219 (2008)
11. Pharow, P., Blobel, B.: Mobile Health Requires Mobile Security: Challenges, Solutions and Standardization. Stud. Health Tech. Info. 136, 697–702 (2008)
12. Simpson, L.A., et al.: Childhood Obesity: The Role of Health Policy. Report to the Second National Childhood Obesity Congres, Miami, Florida (2008)
13. Hufnagel, S.P.: Interoperability. Military Medicine 174, 43–50 (2009)
14. ProjectHealthDesign, Tracking and Sharing Observations from Daily Life Could Transform Chronic Care Management, Johnson, R.W. (ed.) (2010)
15. Kaelber, D.C., et al.: A Research Agenda for Personal Health Records (PHRs). Journal of the American Medical Informatics Association 15, 729–736 (2008)
16. Kendall, D.B.: Improving Health Care in America: Protecting Patient Privacy in the Information Age. Harvard Law & Policy Review 2 (2008)
17. Update: BlueCross ID Theft Warnings Top 5000,000 and Growing. Personal Health Information Privacy (February 22, 2010), `http://www.phiprivacy.net/?p=1993\`
18. Wright, A., Sittig, D.F.: Security Threat Posed by USB-Based Personal Health Records. Annals of Internal Medicine 146, 314–315 (2007)
19. Wright, A., Sittig, D.F.: Encryption Characteristics of Two USB-based Personal Health Record Devices. Journal of the American Medical Informatics Association 14, 397–399 (2007)
20. Simborg, D.W.: The Limits of Free Speech: The PHR Problem. Journal of the American Medical Informatics Association 16, 282–283 (2009)