Impact of Mobile Technologies on Patients’ Health Information Security

Isabelle Fagnot
IESEG School of Management

Follow this and additional works at: http://aisel.aisnet.org/wisp2015

Recommended Citation
http://aisel.aisnet.org/wisp2015/19

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2015 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Impact of Mobile Technologies on Patients’ Health Information Security

Isabelle Fagnot
IESEG School of Management
Paris, France

ABSTRACT

The rate of adoption of mobile technologies or mHealth in the health sector has increased rapidly in the last ten years. This accelerated adoption of information technologies (IT) in delivery of health services and management of healthcare agencies has created an increasingly higher number of associated vulnerabilities such as theft or loss of medical records and human errors. The main goal of this research-in-progress is to study the growing use of mobile technologies in health care (mHealth) and its impact on patients’ health information (PHI) security. The study will also shed light on health practitioners’ attitudes towards security.

Mixed methods will be used to address the questions of this research project. In-depth qualitative interviews of selected participants at health institutions will be conducted. A quantitative study will be administrated to assess the impact of health practitioners’ attitudes on security and to confirm the findings of the qualitative study.

Keywords: Mobile technology, mobile health, patients’ health information, information security, health IT.

1 Corresponding author: i.fagnot@ieseg.fr
2 Annual Report to Congress on Breaches of Unsecured Protected Health Information; 2012 HIMSS Analytics Report: Security of Patient Data
Impact of Mobile Technologies on Patients’ Health Information Security

INTRODUCTION

“NYC Health Center Notifies 1,500 Patients of PHI Data Breach”
“California Facility Reports Two Healthcare Data Breaches”
“Hack at UCLA Health could involve 4.5M people”

These recent headlines relate health data breaches going from having a work laptop stolen with not encrypted patients’ health information (PHI) to a cyber-attack on a university hospital health system. These data breaches in the health sector have been more frequent in recent years affecting more and more patients’ records. Verizon Health Information Data Breach Report reported 1,931 incidents affecting 392 million records in 25 countries.

The rate of adoption of mobile technologies or mHealth in the health sector has increased rapidly in the last ten years. The availability of PHI via mobile applications on various platforms such as tablets, smartphones, and laptops has changed how medical care is delivered to patients. Keeping patients medical information on paper did engender vulnerabilities (medical records loss, misplacement, theft, fire, human error, etc.). This accelerated adoption of Information Technology (IT) in health and the development of digital medical records, if they have limited or suppressed some of the vulnerabilities associated to paper records, have exposed patients digital health information to new forms of information security breaches such as theft or loss of medical records and human errors.

---

7 Annual Report to Congress on Breaches of Unsecured Protected Health Information; 2012 HIMSS Analytics Report: Security of Patient Data
The main goal of this research is to study the growing use of mobile technologies in health care and its impact on PHI security. This research-in-progress examines how mobile technology is used by health practitioners in a group of hospitals, including a teaching hospital, in Europe and the impact mHealth has on PHI security. Such problems are particularly significant in teaching hospitals, which constitute one of the most complex organizational models. This project will use a mixed methods approach: exploratory case study in the qualitative phase (phase 1) followed by an online survey in the quantitative phase (phase 2). This approach will provide a rich understanding of mHealth practices in the group of hospitals. More specifically this project will study the usage and usability of mHealth and what key elements of mHealth security culture may affect overall health information security. The study will also shed light on health practitioners’ attitudes towards PHI security.

BACKGROUND

Mobile technologies in healthcare

Mobile technologies in health care or mHealth is a broad topic and there is no standardized definition of mHealth. For the purpose of this research project, we will use the following definition of mHealth: the use of mobile computing and communications technology in the delivery of healthcare or collection of health information (Kotz, Avancha & Baxi, 2009). By mobile computing and communications technology, we mean laptops, tablets, smartphones and PDAs that provide access to information systems storing PHI.

Health care institutions such as hospitals invest heavily in IT. This investment represents a leadership commitment to enhancing both the quality of care and the productivity of the hospital workforce through the use of modern information
technology resources and services such as mHealth. The rapid development of mHealth presents benefits such as improved quality of care, reduction of cost, enhanced record keeping and mobility but at the same time mHealth has increased security risk (Fernandez-Aleman, Senor, Lozoya and Toval, 2013). One consequence of the increasing use of mHealth and the growing digitization of patients’ data in health care institutions is the emergence of new digital vulnerabilities (Agarwal, Gao, DesRoches, and Jha, 2010) that health care institutions must protect from. A report from HIMSS (2012)\(^8\) showed that the second highest reason of why data is at risk in the health sector is the availability of information on portable devices (31%). It was only 20% in 2010 and 4% in 2008. New forms of vulnerabilities can be the lack of compatibility between devices, loss of connectivity, theft or loss of mobile devices with access to PHI.

**mHealth and Information Security**

The overall security status of organizations such as hospitals does not only depend on its technical elements but also on its behavioral aspects such as employees’ security attitudes and security awareness. Over the years, researchers in the field have argued that vigilant organizations should have highly secure technical information systems together with well-developed policies and procedures to help regulate employees’ behaviors (Stanton, Yamodo-Fagnot, & Stam, 2005).

Another aspect that has an effect on these factors is the rising use of mHealth and with it, the lack of awareness of the users of their security and privacy issues. Schultz (2002) argued that insider attacks are more successful than outsider attacks, and such weaknesses in an organization engender a high cost not only in monetary terms but also with respect to reputation. Stanton, Stam, Mastrangelo & Jolton (2005)\(^8\)

---

\(^8\) Annual Report to Congress on Breaches of Unsecured Protected Health Information; 2012 HIMSS Analytics Report: Security of Patient Data
argued that often security breaches occur because of unintentional mistakes made by employees who lack security awareness. This can become serious when organizations such as hospitals collect, for the functioning of its operations, a significant amount of sensitive information from its patients. The organization is then responsible to insure the sensitive information’s security and privacy (Paquette & Fagnot, 2010).

**METHODODOLOGY**

This research project will use a mixed research approach which will provide a richer understanding of the impact of mHealth on PHI security. This research project is divided into two phases – a qualitative phase and a quantitative phase.

**Phase 1**

For the qualitative phase, the research project will use a case study approach. Case study research method has been used extensively in IS qualitative research (Darke, Shanks & Broadbent, 1998). This approach is particularly appropriate for this research project in security in the health sector as it will to provide a rich understanding of mHealth practices in the hospital. For this research, the type of case study will be exploratory as we are studying a situation that has no clear outcomes yet (Yin, 2003). Selected participants holding medical and/or administrative positions in the health institutions will be interviewed. By medical participants, we mean those involved with patient care for instance doctors or nurses. By administrative participants, we mean those that are not involved with medical practice of patient care such as hospital managers, IT personnel, etc. Please note that on rare occasions it may happen that a participant may be a medical doctor who now holds a fulltime administrative position. Participants will be selected based on their job description and their use of mobile devices in the hospital. It will be important to select
participants with different functions and different levels of interactions with patients and PHI. Participants will be interviewed one-on-one, face-to-face for about 30 minutes using a semi-structured interview protocol. The interview protocol will be based partly on literature and validated protocols. The protocol will also be developed based on the researchers’ experience. The questions in the interview protocol will be open-ended questions. The qualitative data collection will last three months. The data will be analysed using NVivo. The results of the qualitative phase will inform Phase 2 – the quantitative phase.

**Phase 2**

For the quantitative phase, a survey instrument based on the literature and on the results of the qualitative data analysis will be developed. The survey instrument will be designed to further study findings of the qualitative phase. The survey will be distributed to a large pool of hospital employees. Participants to this survey will be selected after the qualitative phase to ensure the most appropriate selection of participants. The survey results should assess whether findings of the qualitative study and the quantitative study correlate. The data will be analyzed using SPSS.

**Research site**

A site for data collection has been secured. Data collection will take place in a group of hospitals, including a teaching hospital, in Western Europe. The data collection is scheduled to start as soon as possible. Discussions are currently on-going regarding the selection of participants for the qualitative phase of the study.

**IMPLICATIONS**

This research study will have implications for both the academic and the practitioner communities. To the academic community, the proposed research will
shed light on the impact of mHealth on PHI security practices. To the practitioner community, this research will provide explanations on the uses of mHealth in hospitals and their impact on PHI security. To this group of hospitals, it will provide a deeper understanding of the practices around mHealth and guidelines on how to keep improving their health and patient information systems. It will inform the hospitals on the attitudes across security issues regarding PHI and how this might impact how we design strategies and evaluate work/task outcomes in the healthcare setting.
REFERENCES


