Mobile Health Requires Mobile Security: Challenges, Solutions, and Standardization

Peter PHAROW 1 and Bernd BLOBEL

eHealth Competence Center, Regensburg University Hospital, Regensburg, Germany

Abstract. Extended communication and advanced cooperation in a permanently growing healthcare and welfare domain require a well-defined set of security services provided by an interoperable security infrastructure based on international and European standards. Any communication and collaboration procedure requires a purpose. But such legal purpose-binding is definitely not the only aspect to carefully be observed and investigated. More and more, aspects of security, safety, privacy, ethics, and quality reach importance while discussing about future-proof health information systems and health networks – regardless whether local, regional or even pan-European networks. During the course of the current paradigm change from an organization-centered to a process-related and to a person-centered health system, different new technologies including mobile solutions need to be applied in order to meet challenges arising from both legal and technical circumstances. Beside the typical Information and Communication Technology systems and applications, the extended use of modern technologies includes large medical devices like, e.g., MRI and CT but also small devices like sensors worn by a person or included in clothing. Security and safety are on top of the priority list. 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 citizens and patients awareness, confidence, and acceptance in future mobile care - a world often still beyond the horizon.

Keywords. eHealth, mHealth, Personal health, security, safety, mobility.

Introduction

Advanced information and communication technology (ICT) solutions are an important pre-requisite for establishing today’s integrated care solutions. Disease management programs (DMP), public health and surveillance systems, and personal care settings are other aspects to be addressed in this context. The ICT infrastructure is hereby a crucial part of the organizational infrastructure as such. While the healthcare and welfare system undergoes the paradigm change from shared care to personal care, the infrastructure needs to undergo a similar migration. It’s not 1970s monolithic dinosaur systems, it’s not 1980s decentralized systems, and it’s not PC-based application environment that may help responding to new challenges. It’s the new world of mobile, and mobilizing, sensors, devices, services, systems, patients and health professionals. The paper aims at addressing mobile health technology security and safety problems.

1 Corresponding Author: Peter Pharow, eHealth Competence Center Regensburg, Regensburg University Hospital, Franz-Josef-Strauss-Allee 11, D-93053 Regensburg. Phone: +49-941-944-6767, Fax: +49-941-944-6766. Email: peter.pharow@klinik.uni-regensburg.de. URL: http://www.ehealth-cc.de
1. Current Healthcare Requirements

The healthcare and welfare systems in all countries around the globe are faced with similar problems. Citizens and patients express increasing expectations while available resources from health funds decrease permanently. In order to cover this funds shortage, patients are obliged to pay more and more services from their own pocket. For an advanced cooperation and collaboration, health networks are established crossing not only borders of domains but increasingly also national boundaries. The society experiences a paradigm change from “Shared Care” towards “Personal Care” requiring advanced communication infrastructures [1]. The care process itself is typically organization-centered meaning that all treatment processes are organized by exactly the hospital or GP the patient has visited. Information exchange is rather rare in this context. Some countries have already started developing a concept of process-oriented care. It’s not a single organization; it’s the disease itself that is in the center of processes including information storage and exchange. All health professionals involved in patient’s care regardless of their affiliation have access to, and provide, case-related medical data items. To meet the comprehensive paradigm of Personal Care, care provision needs to be further developed towards a patient-centered (or rather person-centered) approach moving the citizen into the center of all care processes [2].

This new and enhanced approach needs to invite and incorporate not only health professionals and patients (citizens) but also many new stakeholder groups like, e.g., health politicians, standardization experts, large as well as medium and small (SME) enterprises, professional and citizen associations, chambers, and other organizations. In this respect, eHealth is considered advanced and extended health telematics based on new telemedical technology requiring an extended communication and collaboration. The personalized health (pHealth) provision itself obviously addresses the citizen (patient, client, consumer) being moved to the center of all processes requiring an extended personal and personalized communication among all principals. Mobile health (mHealth) fosters processes to be performed in mobile environment meaning that the network beside traditional applications and systems increasingly contains mobile components (wearable sensors, RFID tags, micro-technology as well as self-organizing components and systems). Communication in mHealth is mainly performed in a mobile network environment [3].

2. Materials and Methods

So what does mobile mean in this respect? What does mobility mean? Is there a sufficient level of awareness, confidence and acceptance among all principals involved for the new levels of health-related security and safety requirements in a speedy world that gets more and more mobile? Is there a technology in place that is promising enough to fulfill or at least strongly support the advanced mHealth requirements?

2.1. Mobile Technology and Mobile Devices

In the virtual world of mHealth, communication and collaboration partners typically do not know each other personally. Increasingly, such communication is performed via protocols for the mobile world (e.g. UMTS). One of the basic requirements is that of a secure, trustworthy, reliable communication using insecure connection means and
media like, e.g., the open and policy-free Internet. Trustworthiness is mainly based on technical mechanisms and algorithms providing communication security services such as identification, authentication, integrity, non-repudiation of origin (authenticity) and receipt, availability and confidentiality as well as application security services such as confidentiality, privacy based on privilege management, authorization, access control, anonymization, pseudonymization but also integrity, accuracy, accountability, auditability and traceability. Identity management (IDM) is a crucial service for most of the aforementioned ones. It includes any actors (persons, organizations, systems, devices, etc.). Other infrastructural services needed are policy and role management.

Devices are among the top priorities in advanced mobile environments. There’s almost no application area in healthcare and welfare without having applied appropriate mobile devices technology. From emergency to treatment to rehabilitation to home-care, personal(ized) medical devices consistently help, among others, treating and monitoring patients at risk or patients at home (see Figure 1).

![Figure 1. Medical mobile devices apply in almost all treatment phases](image)

Quite often especially in the mobile domain, proprietary solutions, outdated approaches, and traditional principles are still in routine use for communicating sensitive information. The awareness level of principals is not significantly high, so real and potential threats and risks are often not addressed. The respective security and risk management is therefore quite weak. Standards like ISO/IEC 17799, ISO/IEC 27799 or the ISO 27000 family are often not known even by professionals [4], [5].

2.2. Patient and Citizen Requirements

The aspect of an active citizen and patient involvement and patient empowerment in the healthcare and welfare processes is an important pre-requisite for achieving the success expected by many developed countries. Health cards and other trustworthy and secure (personalized) devices do play an important role in this process. They allow developing integrated eHealth environments involving health informatics and patient integration. Keywords to foster these processes are health card, secure token and device-related technology but also the role of these tokens and devices in the process of patient integration, their security functionality for data, process and actors’ integrity, the problems concerning access rights, and related data protection and privacy aspects.

From the aforementioned point of view, healthcare systems will increasingly profit from engaged citizens; and engaged patients will have better outcomes. New health
policies, increasing patient needs and decreasing health budgets necessitate patient empowerment. Patient involvement has to take place at different levels within the healthcare process -for example- at the level of care but also at the political level. At the level of care, the interest in citizen engagement is presently changing from past practices -where patient involvement meant that the patient had to go along with the physician’s advice- to a collaborative partnership -where the citizen is considered a real partner within the medical workflow. Also at the political level patient group representatives are increasingly considered valuable partners [6], [7].

2.3. Applied Security Requirements

Secure and reliable communication in a mobile world has applied security requirements coming from different viewpoints. The first one is the “traditional” security domain. Mobile communications address both communication and application security services. But getting mobile definitely brings some important additional requirements addressing, i.e., also electrical, mechanical, and personal safety aspects.

Parameters like, e.g., robustness and self-adaptability is a major key for usability and usefulness in mobile terms, as it is power consumption as well as availability and distance of communication. Mobile devices need to be simple, efficient, handy, and scalable. They need to be safe from electrical, electronic, and personal standpoint. Medical mobile devices need to address these issues, and some other requirements on an even higher quality and reliability level.

2.4. Technical Security Approaches

Mobile communication requires the same -or at least a similar- level of security as ordinary communication using typical infrastructures like LAN or MAN. Thus, mobile security solutions can be based on well-known and well-established symmetric (DES, 3DES, IDEA, AES) and asymmetric (RSA) cryptographic algorithms as well as key traditional exchange protocols, e.g., following the Diffie-Hellman approach [8]. On the other hand, the specific security aspects of a reliable wireless communication require specific modifications in the related protocols, mechanisms, and algorithms. Among others, data to be transferred are typically pre-processed and comprised in order to save time, bandwidth, and power consumption. Micro-technology is therefore used as one of the preferred technologies for advanced security and safety solutions in the context of eHealth, pHealth and especially mHealth.
3. RFID and NFC as a new Chance and Challenge

Radio Frequency IDentification (RFID) and Near Field Communication (NFC) are technical solutions to be applied in healthcare and welfare. Information systems combine ordinary information services with the use of RFID for identifying either goods (drugs, tools, tissues, samples) or even persons (health professionals, patients). Data is exchanged between passive RFID tag and readers in a few centimeters range.

From the health safety point of view, RFID is considered to possibly cause certain health problems. The ubiquitous presence of electromagnetic fields (EMF) is often expected to cause effects of electric or thermic nature to biological systems. In reality, RFID-related EMF values have a considerably low influence on humans. Side effect, however, can appear and shall specifically be considered when pace makers, brain stimulators or other implants are applied. In general, health and personal safety are not affected by RFID and NFC. Nevertheless, technical solutions need specific healthcare and welfare profiles to comprehensively address the health-related safety aspects.

But there’s indeed a problem with RFID as such. Micro-technology is able to deliver RFID tags that are small enough to be provided in liquid even without be noticed by the persons. This is an application area that combines safety aspects and privacy aspects because unexpected and unwanted profiling (tracking) and monitoring will be possible which affects the privacy rights of the persons.

Applying technical standards from other domains in eHealth and mHealth is a challenging task. The US NIST standard, e.g., aims at describing, among others, the applied use of RFID technology in a healthcare environment [9]. Different application fields are identified. They cover asset management, tracking, authenticity, matching, process control, access control, and payment. So many different domains -applying advanced RFID technology- work together forming a supply chain.

4. Discussion of Results and Strategies

Mobile communication often suffers from limited bandwidth. Algorithms pre-process and comprise recorded data. Proprietary protocols do have different serious weaknesses. New protocols and services like, e.g., WPA (Wi-Fi Protected Access), WPA2, and Bluetooth still base on the family of IEEE 802.1x standards but address some of the weak points of the standards themselves and try to overcome the most important drawbacks and pitfalls. Adding a real authentication service (RADIUS) allows for achieving a security level that is (almost) the same compared with ordinary LAN security solutions. The old-fashioned WEP standard is out, WPA und WPA2 address the minimum requirements for a secure mobile communication. These tendencies in the mobile world have significantly influenced the further development of the IEEE
802.11i standard. It’s still a long way to go; the fast application of wireless technology (PDA, UMTS, biomedical devices) has by far not reached its final level.

5. Conclusions

Enhancing mobility has a manifold meaning. It’s not just the use of mobile phones for health-related purposes, and it’s not just the mobility of both patients and health professionals. A mobile environment contains self-organizing systems and components along with mobile devices, tools, sensors, and much more. Patient empowerment means they have to take on their share of responsibility. Citizens have to realize that healthcare is a concern of theirs even while they are not in need of it. This means they have to understand the system. Awareness, confidence, and acceptance range high in future care settings. Standardized and standards-based mobile technology needs to support these processes. Security and safety supports application of new technologies.

The paper addresses awareness of security, safety and quality requirements and solutions in ubiquitous health settings based on the pHealth paradigm. Basic services such as ID management and privacy aspects have been discussed, while services such as policy bridging a still under development.

Acknowledgement

The authors are in debt to the European Commission for supporting and funding the “BioHealth” project as well as other partners and organizations (ISO/TC 215, CEN/TC 251, EFMI WGs CARDS and SSE) for their permanent support and cooperation.

References