Anytime, Anywhere Access to Secure, Privacy-aware Healthcare Services: Issues, Approaches & Challenges

Abstract

A new paradigm, which is at the early stage of inception, is reshaping global healthcare services with emphasis shifting from sporadic acute health care to continuous and integrated health care - an approach being further perfected as anywhere, anytime healthcare services. Recent advances in e-health informatics, digital transformation and remote data exchange, mobile communication, and medical technologies are the enablers of this new paradigm. *Monitoring and on-time intervention*, *integrated care*, *self-care*, and *social support* are four value-added features of anywhere, anytime health care. The already precarious security-privacy conditions of healthcare domain are expected to aggravate in this new paradigm due to lot more monitoring, collection, storage, sharing, and retrieval of patient information as well as collaboration among many different caregivers, institutions and systems. This paper aims to systematically rationalize and explore security-privacy related issues in providing anywhere, anytime healthcare services. We survey the existing approaches and discuss health IT infrastructural governance, institutional and cross-national policy challenges to address the relevant security and privacy issues. We categorize these issues in relation to the users, applications, communications, and devices. A consolidated effort from technological, human factor, and social research communities can lead to an adequate response to key privacy-security issues in this nascent anytime, anywhere healthcare paradigm.

Keywords: *e-Health/m-Health; Security; Privacy; Telehealth; Integrated Healthcare*

[*] Correspondence to: Department of Computer Science, North Carolina A&T State University, Greensboro, NC, USA. *Email:* manwar@ncat.edu (Mohd Anwar).

Anytime, Anywhere Access to Secure, Privacy-aware Healthcare Services: Issues, Approaches & Challenges

1. INTRODUCTION

In recent years, a new paradigm is sweeping across healthcare services at a global proportion with emphasis shifting from sporadic acute health care to continuous and more integrated health care. This shift in approach, characterizing today's healthcare services, may be effectively perfected through implementing and practicing anywhere, anytime healthcare services. The benefits of the integrated healthcare (IH) paradigm include more informed treatment, reduced healthcare cost and higher patient satisfaction.

The IH approach features four key value-added dimensions: *continuous monitoring and intervention, integrated care, self-care,* and *ongoing social and community support*. With e-health informatics advances and the miniaturization of mobile sensors and devices, rapid development and deployment of wireless communication, social computing, and smartphone technology, today's health care is equipped with technology to provide holistic health care.

A first step to preventing acute health condition and mortality is health status monitoring. In 2011, a UK Department of Health reports that remote monitoring cuts patient death by 45%[1]. Indeed, automated monitoring such as blood pressure or high blood sugar can assist patients in managing chronic disease or health conditions. Today, monitoring of basic activities of daily living (ADLs) such as bathing, dressing, toileting, and the like (commonly known as Katz ADL[2]) for the elderly patients has become an essential part of geriatric care, particularly for the aging baby-boomers. Apparently, such monitoring can provide good indicators of the patient cognitive and physical capabilities. Owing to the inability to independently seek health care and their proneness to emergency care, many elderly patients will benefit significantly from active health status monitoring. Oftentimes, when real-time intervention is necessary to maintain good health and wellbeing, lifestyle and activity monitoring can become part of the treatment for the patient.

From an integrated healthcare delivery perspective, the current health services system is largely fragmented. Fragmentation can adversely impact health services quality, cost, and outcomes[3]. Multiple providers are often engaged to offer different services through the different systems. Coordination among systems, services, and providers is therefore key to secured and high quality patient care. While receiving treatment, the movement of patients among multi-provider systems is characteristically not seamless as is desired in an integrated care model. Additionally, while traveling or temporarily residing abroad, a patient's frequent mobility, adds new challenges to well-coordinated patient care.

Self-awareness is precursor to self-management. Currently, the ability of the patients to self-manage their own health is the most desired route towards achieving better health and wellbeing. Living in a global village, we are so well connected with one another and frequently move (travel) from one location to another. As a result, we are exposed to different diseases and are likely to source a variety of services across a series of changing environmental and climatic conditions. In fact, the declining health and wellbeing among today's generation may be attributed broadly to our lifestyle changes with increased exposure to "arm-chair" technologies, for instance, the frequent use of, and engagement with, television programs and computer gaming resulting in a sedentary lifestyle for many people, leaving them little to no motivation for physical exercise or outdoor recreation activities, thereby leading to increased obesity.

As well, social and community support can impact one's health and wellbeing. A health-conscious friend, for example, can exert positive peer pressure on individuals towards inculcating a healthy lifestyle (and habits). Friends, relatives, and social circles also play significant roles in the wellbeing of one's mental health. Indeed, the value-added emotional or informational support or companionship will often help reduce unnecessary psychological distress. Patients with chronic or terminal illness have found engaging with appropriate social media through the sharing of each other's experience to be beneficial [64].

While automated monitoring, integrated care, self-care, and social support can effectively support IH services, as epitomized by anywhere, anytime healthcare services, the main challenge for practicing this approach lies today in the security-privacy aspects of such services. Without ensuring the security and privacy of such services, they will fall apart eventually due to non-acceptance by end-users and/or failure to comply with security-privacy legislations. Moreover, abuses and misuses of such services can systematically cause harm of many forms, from minor inconvenience to financial loss to major injury, even towards death. Similarly, breaches of patient health information security and privacy in routine (and/or non-routine) data exchanges or transmission can dangerously victimize a patient (i.e., becoming a victim of embarrassment, prejudice, discrimination, and more).

Notably, IH services sustainability will depend chiefly on the assurance of service compliance with privacy-security mandates as legislated by the different countries where such practices are to be performed, as well as guiding such practices based on commonly established principles dictating the protection of personal data privacy and security, particular the cross-border flow of sensitive health data. Hence, our contribution here will be three-fold: First, we present a holistic approach to information and communication technology (ICT)-based anywhere, anytime healthcare paradigm; second, we explore security-privacy issues and review their considerations within the new IH paradigm; finally, we discuss existing approaches and report on health ICT infrastructural governance, institutional and cross-national policy challenges to address the key security-privacy issues.

The general layout of the paper is as follows. Section II characterizes a scenario of anywhere, anytime healthcare services. Section III presents security-privacy issues related to realizing IH paradigm. Section IV surveys potential approaches to address security-privacy related issues and inherent challenges faced by anywhere, anytime healthcare services to be practiced within and, when needed or where possible, across the boundaries of different countries. Section V presents concluding remarks.

2 ANYWHERE, ANYTIME HEALTHCARE SERVICES

More recently, the ease and convenience of receiving health care from anywhere and at anytime has become possible with advances in e-health informatics, sensor technology, and mobile devices (e.g., smartphones). Central to this approach is the consideration of health and wellbeing throughout a person's lifetime. As aforementioned, four added-value features of this approach include *monitoring and on-time intervention, integrated care, self-care,* and *social support*, each of which brings unique challenges and issues regarding the delivery of safe, secure, and privacy-aware healthcare services.

2.1 Monitoring Devices & On-Time Intervention

Owing to the rapid miniaturization of devices and advances in wireless technology, use of monitoring devices for tracking health conditions is on the rise. Today, a system of remote sensors, spanning one's body or residence can be conveniently networked to monitor one's physical or environmental characteristics. Such monitoring can aid in identifying the susceptibility of certain diseases in a particular population, area, or environment. It is also essential for early interventions, for example, when alerted to the onset of certain diseases and/or being mindful of one's deteriorating health conditions. Through early diagnosis and care, significant long-term healthcare expenses may also be reduced.

Monitoring (and on-time intervention) are beneficial in at least three (3) main areas: (a) lifestyle and general wellbeing monitoring (e.g., daily weights, heart rate and rhythm while exercising); (b) chronic disease or condition management (e.g., cardiac arrhythmia, diabetes, chronic pain); and (c) clinical workflow management such as telehealth or face-to-face care activities (e.g., in-patient care workflow). Two types of health status monitoring devices have been deployed: in-body (implanted) devices, and on-body (wearable) devices. Implanted devices (e.g., pacemakers, defibrillators, and neurostimulators) monitor and treat physiological conditions within the body. These devices have wireless capabilities that enable remote monitoring of the patient's health status through an implant reader which can later forward information over the Internet to the caregiver. Wearable devices include motion sensors and blood pressure meters, which are often used to aid lifestyle and general wellbeing monitoring. Besides health status monitoring, user environment also needs to be monitored to ensure wellbeing. Examples of such environmental monitoring include the normal daily routine monitoring of seniors such as ADLs, and the environmental triggers monitoring for asthma.

Nowadays, radio frequency identification (RFID) technology is commonly employed to monitor medical assets and personnel when there is a need to provide immediate care. For example, when patients seek emergency medical attention, a health professional may need to be aware of implanted devices. In this instance, an emergency doctor treating a patient who has an implanted pacemaker while suffering from heart attack can attach RFID tags to the implant for device identification. It would be convenient to have the RFID reader give the doctors immediate access to information about the pacemaker. To achieve this, a near field communication (NFC) chip-embedded in a mobile phone can act as an RFID reader when the phone is turned on.

Once patient health information is collected, healthcare providers must store it in a way that is easily and quickly accessible only to authorized personnel. As maintaining an ICT department to keep the patient information digitally stored in a secure server can be costly for both small practices and/or for complex management of such information treated in a multi-provider organizational setting, outsourcing of health information management to cloud providers has emerged. Health clouds provide access to stored records quickly and conveniently from anywhere at anytime. Further, as organizations grow, cloud vendors can often provide infrastructural scalability as and when needed. With all the different monitoring devices, affordable storage devices, and cloud infrastructure, health providers will quickly amass volumes of "sensitive" data. These data are often heterogeneous in structure and character, but have the prospect to spur innovation and enhance our understanding of patient care. Owing to increased health data exchanges, "big data analytics" are now needed to search, share, analyze, or visualize such data, especially if the original data are also somehow "linkable."

2.2 Integrated Care Model

Typically, a patient's treatment may involve a physician visit followed by an assigned diagnostic lab procedure before filling a prescription order at a local pharmacy. Additionally, the physician may require access to information (i.e., the patient health history) held by other caregivers. Thus, no single caregiver can cater to all of an individual patient's needs. Given that a patient's health information is often fragmented and/or dispersed across multi-provider systems, proper coordination (and integration) among the different caregivers is essential to properly care for a patient.

When sequencing healthcare services, there often is the need to coordinate different services with the patient's health information passed from one preceding service provider to the next. For example, a patient's surgery is often preceded by anesthesiology service and followed by a post-operative care, which may further be followed by a rehabilitation service. In this instance, access to a patient longitudinal record of say, the treatment history, will allow each care provider of the patient access to key relevant information at the point of care. For patients having multiple disease complications, the accessibility and availability of such a comprehensive set of records at the point of care will be even more important if the patient's conditions and respective medical interventions for one illness are to be considered while being treated for another condition.

In today's highly connected world, the increased mobility of patients has also significantly increased healthcare services needs for geographically dispersed locations. This is true especially with people who make frequent trips to countries other than where they may be receiving primary care services. In November 2010, over 1.6 million people traveled from the US to Canada. Among the frequent travelers are elderly patients and those with chronic health conditions who may need frequent checkups and follow-ups. As a result, even cross-border healthcare integration is creating a data sharing challenge. Healthcare providers must now understand how the Internet and ICTs integrate with and extend on-site health facilities. Nationwide health information network (NHIN)[4] is one such initiative underway towards information sharing among federal agencies, hospitals, and doctor offices. In the near future, it is likely that on-site and online health services will become more blended so that anyone can receive health services of their choice from any facility, locally or remotely.

Essentially, workflow in healthcare is viewed as a key technology for integration. Integration between health services and wellbeing services is needed to aid people, communities, and even subsets of a country's population to live and maintain a healthy lifestyle. An integrated care model can be achieved by consolidating healthcare services and workflow in healthcare via a horizontal vs. vertical integration. In the former, independent healthcare providers collaborate towards accomplishing a broader goal (e.g., integrating hospital and nursing homes). In the latter, interdependent service providers combine and coordinate efforts through proper information exchange and information management (e.g., integrating primary care and specialty care). Both types of integration interconnect services to enable seamless and continuous care.

2.3 Self-Care

Self-care is a first step to living a healthy life, the first response to a health problem. As noted in the Encyclopedia of Public Health[5], support for self-care behavior has the potential to significantly improve an individual's health and wellbeing with instances of self-care behaviors to encompass: (1) seeking relevant health information and evaluating the advice sought via lay and/or alternative care networks; (2) regular monitoring of one's own health and vital signs; (3) maintaining a healthy lifestyle and/or performing healthy lifestyle activities such as adopting a healthy and low fat diet, smoking cessation and exercising; and (4) making informed decisions about one's own health. Seeking health-relevant information and self-education include reading books or pamphlets on health and wellbeing, attending classes and/or searching the Internet for specific healthy lifestyle related topics, as well as seeking advice from trustworthy care practitioners and/or joining a self-help group.

Since personal health record (PHR) is the *prima facie* observation by an individual about his/her own health, it is at the center of self-management of personal health. On the one side, PHR can provide users with information resources to understand their personal health; on the other side, decision-support tools can be integrated into the PHR to aid users make health-promoting lifestyle choices and activities to support self-care. Examples of current PHR systems include Microsoft's HealthVault[68], The Patient Portal[67], MyChart[66] and MyOscar[65]. One 2008 study estimates that as many as 70 million people in the US have access to PHR systems[6]. Once entered, a PHR system uses the information to provide users with a merged health record, comprising information on conditions, and possible interactions among prescribed drugs, conditions, and allergies. Patients may also maintain their health records in portable storage devices (e.g., USB keys) or transfer health information from wearable monitoring devices to Bluetooth-enabled devices such as PDAs, cellphones, or smartphones.

Web-based applications for self-management of chronic diseases are gaining popularity (e.g., the diabetes management program described by Lorig et al.[7]). Many organizations and agencies (e.g., organization of medical librarians[8], Harvard Health[9], HelpGuide[10], etc.) maintain credible web health resources (blogs, tools, illustrations, videos). New frontiers for improving personal health and wellbeing include smartphones and tablet applications, colloquially known as “apps”. Smartphone apps are possibly the best and most convenient way of reaching people anywhere at anytime. These apps offer health assessment (e.g., BMI calculator), health activity analysis (e.g., RunKeeper[11] for GPS activity tracking during sport), awareness (e.g., CDC Vaccine Schedule, Outbreaks Near Me – notifies users of outbreaks of infectious diseases worldwide), education (e.g., SleepBot – graphs and analyzes sleep patterns), and even administers treatment (e.g., WebMD for iPad).

2.4 Social support

Social media[12] (e.g., blogs, tweets, wikis, online social networks or OSNs) can become the enabler of social connectedness. By and large, social connectedness and social support are useful mechanisms to help maintain good health, with support coming from friends, family, acquaintances, or even strangers. Peer pressure can influence individuals to develop healthy lifestyle habits with health conversation and health information sharing taking place within OSNs.

Collective knowledge of users may provide unique insight into particular health issues, for example, websites such as patientslikeme.com allow users to share personal experience, become more informed about one’s symptoms and conditions while learning from others. Overall, OSNs can be valuable in facilitating the promotion of healthy lifestyle activities such as having family members and friends track each other’s health activities, provide encouragements and/or exert peer pressure to help individuals stay on a healthy lifestyle track. BodySpace[13] is an example of a social fitness and weight- loss application. Ultimately, the purpose of these Web-based social communities is to assist patients and their families to make more educated health choices. Yet, health *mis*information may be dangerous if and should the wrong health advice be offered.

Smartphones and other mobile devices boost social networks. Using these devices, for example, an elderly or an infirm can constantly update their health status through tweets via Twittter[14]. According to Domingo[15], healthcare social networks provide an attractive platform for sharing ideas, discussing symptoms and debating treatment options. OSNs mimic offline word-of-mouth (WOM) communications, implying that health information may spread quickly even among OSN users who are not directly connected.

Today, health-related OSNs are gaining increasing popularity while general-purpose OSNs such as Facebook are serving as pervasive outlets for health messages. FatSecret[16], for instance, is a free OSN service for people who are interested in food and diet. As a community, FatSecret enables its users to share cooking recipes, follow popular diets, and take up challenges together with other users (such as "Do not eat after 8pm").

Aside from OSNs, an individual patient's blog post-chronicling the personal experience on fighting a debilitating disease such as breast or prostate cancer can be very helpful to another patient. Likewise, a caregiver's blog with postings on professional experience in dealing with patients with specific chronic health conditions can help another caregiver.

One emerging means to supporting social wellbeing is gaming. One such project to create virtual immediacy between long-stay absentees and their primary social contact group is Scottie[17], whose target users are primarily hospitalized children who have a need to maintain their relationships while being away from home.

3 Security & Privacy Issues

At this point, we shift focus to key security-privacy issues in the context of the IH paradigm. In and of itself, health information is privacy-sensitive. When President Clinton introduced HIPAA, he remarked that "Nothing is more private than someone's medical or psychiatric records"[18]. Security vulnerabilities in healthcare delivery systems may cause various consequences to patients including the denial of service to death. For service providers, security vulnerabilities can lead to legal sanctions, financial loss, or loss of reputation. Indeed, owing to the significant increase for information sharing among multi-providers to coordinate "care" within an integrated care model, security-privacy issues have become quite complex. Moreover, some issues may have more impact on one particular feature of this paradigm than another, for example, issues of device and communication security will be more prominent in monitoring and on-time interventions whereas application security issues are likely to be more conspicuous in self-care.

Figure 1 categorizes security-privacy related issues in IH paradigm into four planes: *user, application, communication, and device.*

3.1 User-Plane Issues

At the user level, security-privacy issues originate typically from the preferences, perceptions, and abilities of the respective users. With demographic profiles, physical and mental abilities of patients being different for different users, privacy-security issues are thus be quite different for different individuals, resulting in the need to address different types of attacks.

3.1.1 User Privacy Issues

Different patients perceive privacy differently. As healthcare domain covers patients of different race, color, culture, age groups, moral and ethical values, patients have widely differing privacy preferences. As Berendt et al.[19] noted, some patients may be *privacy fundamentalists*[69] (concerned about disclosing any data)*;* some may be *marginally concerned*[69] (willing to provide data under almost any condition)*;* others may be *profiling averse* (concerned about disclosing interests, hobbies, health status, etc.) while some others may be *identity concerned* (concerned about revealing identity information such as name, email, address, etc.).

3.1.2 User Security Issues

Securing health information may not be the immediate concern of a patient. Patients would not restrict themselves from using any service as long as they perceive health benefits resulting from it. A 2011 Pew Internet & American Life Project[20] survey reports that 80% of Internet users search online for health information. As a result, the phishing attacks targeting users seeking online health information are very likely to be successful. Many patients are not technically savvy to understand the potential risks and security consequences of using health-related tools, applications, and services. Health conditions may create added safety risks for patients when using a particular health application or device, for example, hackers were found to assault epilepsy patients on the Epilepsy Foundations online forums by embedding flashing animations designed to induce epileptic seizures[21].

3.2 Application-Plane Issues

At the application level, as they would have used some health applications to perform a variety of tasks, end-users (i.e., patients, caregivers, researchers, or friends and family of patients) are most familiar with security issues. Privacy-security concerns of smartphone apps and third party apps of OSNs in health care are looming due to the ubiquity of smartphones and popularity of OSNs reaching out quickly to a massive number of users.

3.2.1 Application Privacy Issues

Most of the healthcare applications send, or have the capability to send, data from user computers to the application servers. Generally, the application users have no clear idea about what information is being transmitted, or who may be the recipient of the transmitted information.

A recent study[22] reported that out of an examination of 101 popular smartphone “apps” (games and other software applications for iPhone and Android phone), 56 of these apps transmitted the phone's unique device ID to other companies without the users' awareness or consent. 47 apps transmitted the phone's location in some way while 5 of them sent age, gender and other personal details to outsiders. Many developers offer apps for free, hoping to profit by selling ads inside the app. These apps transmit users' locations to advertisers so that ads can be targeted by location, which is a clear breach of location privacy. Furthermore, sometimes apps share age, gender, income, ethnicity, sexual orientation and political views of the application users to advertisers. Google, for example, discloses in its privacy policy that it may use information from user profiles to customize advertising[23].

3.2.2 Application Security Issues

Today, the majority of personal health applications are developed for smartphones and tablets. However, the protection mechanisms for such applications are often inadequate. For example, Android allows applications (or developers) to specify the policy that govern access to their interface or data during the install time; yet, the application has limited ability thereafter to govern to whom those rights are given or how they may be exercised[24]. As a result, a mobile health (mhealth) app may inadvertently allow a malicious application to access its interface or data or vice-versa for extending their features and offering more capabilities to users.

SMS phishing (also known as SMiShing) is on the rise as reported by McAfee Avert Lab[25]. A malware may pose itself as a benign healthcare app and may access text messages, contacts, videos, phone transcripts, or call history. Malware can use text-messaging APIs to send fake messages to people in contact list or block messages. Using mobile voice-recording API, a malware application may turn smartphone into a tape recorder. Au et al.[26] pointed out that application developers request more information than what they need for the application and hence breaches the principle of least privilege.

Health-related OSNs or virtual communities (VCs) are increasingly deployed as social support tools for health and wellbeing. Sometimes OSNs and VCs serve vulnerable patients whose safety risks are much higher than others, for example, patients who have been sexually abused or are mentally retarded. Since an OSN or a VC is a web-based service, it consists of several components, namely, client-side code, server-side code, application server, and web server, with the security vulnerabilities embedded in any of these components.

These vulnerabilities often imply that the attackers will be able to hijack user sessions; deface websites; possibly introduce worms; access unauthorized resources; conduct identity theft; and more. Sometimes these web-based services use web-tracking and information-gathering technologies to allow service providers and marketers to collect huge amount of consumer information even without the knowledge of the end-users. For example, a recent finding reports that Facebook tracks users every move on the Web even when they logged out[27].

3.3 Communication-Plane Issues

At the communication level, key issues include: (a) when devices interact with each other; (b) when information collected by a remote device is communicated to caregivers; and (c) when a caregiver remotely communicates with the device to execute certain commands. In order to achieve better treatment and/or render more appropriate care, patient data (e.g., habits and intimate details of their health conditions) often need to be transferred from the monitoring devices to a caregiver. Alternatively, one caregiver needs to pass on the collected information in a patient health record to another caregiver. Altogether, patient health information is oftentimes automatically transferred among devices and individuals in the process of delivering health care. In such a communication set up, sensitive health information is subject to privacy breaches and security attacks.

3.3.1 Communication Privacy Issues

Sometimes health information is self-reported and sometimes it is propagated to healthcare provider through multiple communication channels. When en route, flow of information may be observed, which can result in the discovery of the treatment of a particular patient by a particular provider for a certain condition. By tracking communication between source and destination nodes, patient as well as provider locations can be easily tracked, thereby breaching their location privacy.

3.3.2 Communication Security Issues

The communication channels that connect nodes (e.g., patient and healthcare provider) may be implemented using various physical media and communication and routing protocols. The security of media, signal, and binary transmission of data are often termed as physical layer security. The physical data medium may be wired such as copper wire, co-axial cable and fiber-optic cable and/or wireless such as infrared, microwave links and cellular mobile networks, or via satellite. The physical layer of networks needs to withstand different types of attack including jamming, eavesdropping and interception.

Most of the monitoring devices are designed to communicate with healthcare providers and/or health-intervention systems automatically, remotely, and wirelessly. For example, pacemakers, defibrillators and insulin pumps emit wireless signals. In addition, for many geriatrics care cases, each user carries more than one device or sensors that are also connected to the same network and interoperate among them. Thus issues of communication security in wireless network can become very prevalent in a growing (and sensitive) healthcare network.

On the one hand, by sensing emanation, signals transporting through the wired medium might be captured; on the other hand, as wireless transmissions inherently broadcast without physical boundary, any receivers nearby may be able to pick up the transmission. Accordingly, issues of physical layer security in a wireless network will be more prevalent than in a wired network. Bluetooth is the most popular wireless medium for personal medical devices. It is widely used for most of the mobile health sensing applications[28]. Bluetooth is susceptible to man-in-the-middle (eavesdropping or interception) attacks, battery depletion attack, and device-discovery attack[29].

Once a physical medium is compromised, hackers can access and remotely control medical devices like insulin pumps, pacemakers and cardiac defibrillators, all of which emit wireless signals. An adversary may change device settings to change or disable therapies (integrity attack). Furthermore, an adversary may overflow a device's data storage media or constantly send command signals to drain a device's battery, which is also knows as "sleep deprivation attack". Some metadata of Internet communication (e.g. email address, IP-address, HTTP cookies) and traffic analysis become significant threats to the confidentiality of personal data.

Wireless channels can serve as a portal to launching security attacks. With only the users manual and some publicly available information, such as the specifications of the radio chip used by the insulin pump, authors in Li et al.[30] were able to eavesdrop on the wireless communications using off-the-shelf hardware and a publicly available software radio platform. Furthermore, after reverse-engineering the communication protocol and packet format, they were able to fully discover the device PIN of the remote control and glucose meter, and regenerate a legitimate data packet, which is accepted by the insulin pump, containing misleading information, for example, an incorrect reading of the glucose level, control command for stopping/resuming of insulin injection, and control command for immediately injecting a dose of insulin into the human body.

Using an antenna, radio hardware, and a PC, Halperin et al.[31] found that someone could violate the privacy of patient information and medical telemetry. The adversary's computer could intercept wireless signals from the Implantable Cardiac Defibrillators (ICD) and learn information including: the patient's name, the patient's medical history, the patient's date of birth, and so on. Moreover, someone could also turn off or modify therapy settings stored on the ICD.

Since multiple types of short-range wireless technologies (Bluetooth or Zigbee) are used simultaneously within close range inside a healthcare setting, the potential for interference among them and with medical devices also becomes a concern[32]. In a dense wireless environment, multiple short-range communications at the same frequency may cause electromagnetic interference on the communication channel resulting in significant data transfer latency and data loss.

3.4 Device-Plane Issues

At the device plane, privacy-security issues are pertinent to situations where some monitoring, storage, or therapeutic devices are being used. The presence of a vast number of medical devices has complicated the security landscape in the healthcare domain. In fact, at an estimated US$133 billion by 2016, the US medical device market is the world's largest[33].

3.4.1 Device Privacy Issues

As it is possible for a wearable medical device to give an unwanted exposure to a person's health status, an easily exposed wearable device always run the risk of privacy breaches. Sometimes, mere exposure to a device may not be a concern, but the identification of the type of device may reveal a specific condition. A patient may be sensitive about disclosing certain condition, which may have social stigma. Since a device is co-located with the patient, an ability to track such a device can easily reveal the presence and absence of a patient in a particular location. Thus, the ease of tracking a device also raises the concerns over location privacy.

3.4.2 Device Security Issues

Device security issues could be mechanical or software-related. Software defects in medical devices abound: during the first half of 2010, FDA reported at least six software-related device recalls[70]. Here, our focus is on the device security issues related to software, often called firmware. Medical devices are predominantly controlled by firmware. These firmware programs usually run on privilege mode to interpret and display sensor information in monitoring devices (e.g., heart rate, blood pressure), dispense medication (e.g., blood, saline), analyze raw data to create human-understandable images (e.g., CT, CAT scan), deliver therapy (e.g., cardiac pacing and defibrillation), and/or respond to changes in a doctor's intervention.

An adversary can launch attacks on devices by exploiting defects in firmware. Simple examples of firmware defects in devices include buffer overflow and inconsistent error handling. An adversary may compromise confidentiality, integrity, or availability of data collected by these medical devices. In confidentiality attack, the adversary gains illegitimate access to these devices. As a result, the adversary may have access to patient identification data as well as medical records such as ECG waveform, blood pressure, heart rate, treatment information (e.g., flow rate or volume delivered in an infusion pump), and so on. In an integrity attack, the adversary can change the data maintained by these devices. An adversary can also make these devices inaccessible to authorized user by launching availability attack (e.g., sleep deprivation attack).

Data availability and integrity are essential in providing timely and quality healthcare. Medical devices can become easy targets of insider attacks. Insider adversaries may include clinicians, software/hardware professionals, and/or even patients themselves. Since RFID tags have been used widely to identify implantable devices, eavesdropping on RFID readers is a major threat to implanted devices. An eavesdropper with an antenna and some basic receiving equipment can easily gather RFID tag information. As a result, a patient with implanted devices can become a victim of stalking and other crime.

4 APPROACHES & CHALLENGES

Unique challenges exist to address privacy-security issues at user, application, communication, and device planes in anytime anywhere healthcare paradigm. In **Figure 2**, we list the approaches to address these problems, as well as the challenges in addressing these issues.

4.1 User Plane

4,1,1 Human factor analysis.

The efficacy of any technical solution to security depends partly on the assumptions made about the end-user (i.e., patients, patients' next-of-kins, employees of the healthcare organizations, and so on) behavior and their physical and cognitive abilities. Essentially, an analysis of end-user security behavior and its implications is the important first step to validate these assumptions. For example, Stanton et al.[34] propose a two-factor taxonomy of end-user security behaviors. These two factors are: intentionality of security behavior and security behavior requiring technical expertise. For example, choosing a bad password is a security behavior that requires minimal technical expertise and neutral behavioral intention.

Importantly, an organization needs to promote good behavior and restrict bad behavior of end-users in order to make technical solutions effective. An example of bad security behavior is the case of healthcare professionals carrying patient information on their smartphones that are not adequately secure. As well, the mental and physical abilities of end-users play a significant role on the effectiveness of a technology. For instance, the effectiveness of a password-protected system lies in the ability of an end- user to remember a complex password; otherwise, an expressive access control policy tool would not do any good to the users if it were a cognitive burden on them to author such a policy.

Altogether, time and complexity involved in a security procedure sometimes determine the acceptability of that procedure. Also, the physical ability of a patient may sometimes be an impediment to the use of a security device, for example, some researchers propose carrying a device by the patient to fend off attack on her implanted devices[35], a solution unlikely to be acceptable to a senile patient.

4.1.2 Social factor analysis.

As for non-technical vulnerabilities, information assurance (IA) goals of the healthcare organization should and need to be first identified. Next, these established IA objectives would have to be realized through mandated policies and procedures.

Social factor analysis can help elucidate IA objectives. Social factor like reputation of the organization is one of the drivers for setting organizational IA objectives. The codes of conduct within the healthcare organization need to be cognizant of ethical, privacy and security implications. Social and cultural values of the patients determine their desired level of security and privacy. Since privacy is an expectation of a patient about how their health information will be handled and used, the organization has to implement the online security and privacy solutions to meet those expectations. Typically, ongoing monitoring is generally presumed to maintain the trusted private and secure online service environment, and predefined procedures to address emergency situations like security attacks must be readily available to be activated when and if necessary. Further, healthcare providers need to practice transparency and accountability to increase patients' confidence over the security of the data.

Security policies and procedures are always challenged by human and social factors. For instance, difference in legal systems may cause some technical difficulties such as interoperability as well as the legal status of digital signatures across various countries[36]. For example, a 2013 OCED study suggested the need to strengthen health information infrastructure to achieve quality healthcare governance[37]. Essentially, while OECD privacy guidelines offer a framework to collectively develop national data protection legislation, significant differences in the application of these principles across countries create impediments for building cross-country databases, the ability to link and share data and care collaborations. In fact, many countries, including even developed countries such as Finland, Canada and the US still face concerns about the legal authority to build databases from electronic health records (EHRs) and use of "personal data" within such EHRs, pending further significant legislative reforms.

As a result, coordinating treatment of a patient who is visiting outside of his home country may not just be difficult, but sometimes ethically and politically complex. Besides, it is hard to set objectives and policies that address all the patients associated with all the different scenarios. Organizations have to be ready to make adjustments and changes in their security policies as they adopt new technology or face new security and privacy breaches.

4.2 Application Plane

4,2,1 Security Testing.

The commonly applied testing for software security is penetration testing. Penetration testing is effective when security is considered early on the software development process and test activities are based on the findings during the requirement analysis, architectural risk and more[38].

As security is often not considered a feature prior to the development of a health application, it is either not tested for security or it is tested very late on the lifecycle when the security flaws cannot be easily fixed. Moreover, sometimes health applications are developed as mashups. But some of the components of a mashup may not be developed with security in mind. In such an event, security testing cannot adequately address the security flaws in the applications.

4,2,2 Design by Contract

The design by contract methodology requires a module whose input satisfies its preconditions to produce an output satisfying its post-conditions, contributing towards the development of software that will function well in its intended environment. However, in any sufficiently complex piece of software, it is not possible to guarantee that all contingencies will be addressed in a specification, or all modules will properly meet their specifications under all conditions[39].

In integrated care scenario (e.g., workflow system), or a scenario where health applications are developed wiring different components (e.g., mashups), design by contract methodology is hard to enforce. In addition, as a module's behavior is undefined when its preconditions are violated, the design-by-contract interface may provide an attacker insight (violating precondition) to launch an attack.

4,2,3 Secure Design Principle

The Secure Design principle states that every program and every system user should operate using the least set of privileges necessary to complete the job[40]. The idea is that the applications running with restricted privileges will not have access to perform operations that could result in high-impact security breaches. Yet, some platforms (e.g., Android) do not properly support PLP and users of some platforms (e.g., Windows) do not understand how to take advantage of PLP.

Davi et al.[41] showed that Android's permission mechanism is deficient to restrict a non- privileged caller application to access components of a privileged caller application, better known as privilege escalation attacks. Motiee et al.[42] reported that at least 69% of their 45 study participants violated the PLP by not properly using user account control of Windows Vista and Windows 7. As a result, PLP is not enforced to restrict many of the malicious self-care health applications developed for end-users.

4,2,4 Access Control

The access control mechanisms used in health care are often bypassed in case of emergencies, colloquially known as "break- the-glass". Malicious users can exploit the break-the- glass principle to gain unauthorized accesses. Even though, there is some effort to regulate break-the-glass exceptions[43], the exception is still subject to abuse.

4,2,5 Data Masking

Data masking techniques, such as k-anonymization or microaggregation are popular solutions to privacy violation when healthcare providers share patient information with external organization for research, analysis, or any other reasons.

Owing to widespread use of health status monitoring technology (i.e., health monitoring devices, which sense so much patient health information) and data collection tools (i.e., EHRs and PHRs), healthcare providers have been generating terabyte data. However, most of the current anonymization algorithms have been devised to work with small sets of data.

A study by Aggarwal[44] showed that when the data contains a large number of attributes, which may be considered quasi-identifiers, it becomes difficult to anonymize the data without an unacceptably high amount of information loss. Besides, the optimal solution for microaggregation is known to be NP-hard[45]. However, it is important that the anonymization techniques have to protect identification of individual health records while keeping the data useful for research and analysis.

4,2,6 Cryptographic Protocols.

Several cryptographic schemes[46,47,48] based on attribute-based encryption (ABE) have been proposed in the literature to preserve the privacy of electronic medical records (EMRs). Still, these works do not address issues such as cipher-text overheads on records, encryption/decryption efficiency, and key and policy management that one would face when deploying these cryptographic schemes.

Akinyele et al.[49] provided a design and proof-of-concept implementation of self-protecting EMRs using attribute-based encryption on mobile devices. One of the design challenges of ABE is on what attribute a user should be allowed to access a medical record. One of the main weaknesses is the lack of anonymity, as user must reveal his identity to the system. In a health scenario that requires quicker response, ABE may not be a good procedure to achieve break-the-glass exception.

4,2,7 Secure End-User Education

A study by Dhamija et al.[50] identified that the lack of knowledge (of computer systems, security, and security indicators) is one of the three reasons for why people fall prey of phishing attacks.

Today, evidence exists to support the idea that well-designed user security education can be effective in the real world[51]. However, the user will always circumvent a security model where the security features clash with the tasks the user is trying to do[52]. As a result, user-based protection mechanisms are always fragile. Besides, some patients, especially those who are aging and elderly, may not be receptive to education due to age, health, mental, and other limiting conditions.

4.3 Communication Plane

4,3.1 Virtual Private Networks (VPN)

To keep the data exchange confidential and unchanged in transit, the healthcare VPN uses access control and encryption technologies to simulate a private network over a public network such as the Internet. Today's healthcare solutions rely on different types of wireless and ad-hoc opportunistic networks, where data transmission speeds are slower and signal strengths are weaker.

VPN tunneling can further slow down the transmission. The time required in performing encryption at a VPN concentrator and decryption at the client side video adds significant overhead to the transmission of real-time video, which is already delay-sensitive. A study by Park et al.[53] showed that VPN-based encryption introduces significant latency to real-time video. Viruses and worms can pass through VPN into institutional network and a virus-infected mobile device can spread it to the whole network rapidly[54].

4,3.2 Intrusion Detection (IDS).

While encryption, authorization, or authentication are the first lines of defense against security and privacy attacks, intrusion detection is the second line of defense. By taking control of a sensor node, an adversary gains access to cryptographic keys and access privileges.

Giani et al.[55] proposed anomaly detection based IDS for wireless sensor network (WSN) for healthcare systems. Even so, applying IDS to health WSN faces multiple challenges: (1) multiple sensors create multiple points of attack; and (2) IDS program in every sensor node may not be practical due to general constrained resources.

4,3.3 Message Authentication & Handshake Protocols

Message authentication techniques allow communicating parties to verify the authenticity of each other as well as the content of their message to ensure that the message is not modified or retransmitted. In a computationally constrained health WSN, it is more practical to use message authentication code (MAC) than cryptographic schemes to verify authenticity of message. There have been some efforts[56,57] to develop efficient and compact MAC implementation for a computationally constrained environment.

4,3.4 Electromagnetic (Monitoring) Interference (EMI)

To avoid communication device induced electromagnetic interference on another communication device, especially if the communication device is also a medical device, a cautionary choice needs to be made on communications that are allowable and required. This is especially true for communications among critical medical devices within a certain area in a physical space.

Healthcare providers have to consider the patients who are, or will be, exposed to the environment of interest, taking steps to prevent interference on critical medical devices, and monitor for EMI to identify when medical device interference occurs.

4.4 Device Plane

4,4.1 Device Encryption

Several cryptographic approaches[58-61] have been proposed to restrict online access on implanted medical devices (IMDs). One key concern, however, is that healthcare professionals always needed to have immediate access to implanted devices. If a device has embedded cryptographic methods in it, the health professional without proper credential would not have access to that device. As a result, it would be an impediment to treating the patient if and while the patient is traveling and encounters an emergency situation.

Encryption is the best available way to protect local device data from offline hardware attacks. For instance, full disk encryption (FDE) can protect data in the situation when data is read directly from hardware without OS mediation. Even though hardware-based FDE can provide the best protection, not all devices (e.g., smartphone devices) offer FDE.

4,4.2 Fail-Secure Device Design

In the event of a failure, a “fail-secure” medical device is designed not to leave sensitive patient data embedded in the device in an insecure state. Put simply, the device design has to mitigate the security consequences of the device’s failure.

Fail-secure design requires the analysis of system behaviors resulting from component failures. A method to identify potentially undesirable information flows based on the fault modes of the system’s components has been proposed by Rae et al.[62]. Nonetheless, an exhaustive evaluation of faulty behaviors in a device can be quite complicated because (1) some behaviors may result from the failure of individual components; (2) some may result from the sequential or concurrent failure of a set of components; and (3) some others may result from the overall design flaw.

4,4.3 Device-Level Trust & Access Control

Based on the purpose of use and security vulnerabilities, one device may be trusted differently than or from another. In a pervasive healthcare environment (e.g., smart-home health environment), many devices will be used and will interact with each other. An attacker may compromise one such device to launch attacks on other devices.

In addition to users, devices may be assigned privileges to access resources owned by other devices. For instance, Bussard et al.[63] offered a trust model for device-level authorization in a pervasive business-to-employee scenario. In most cases, however, a healthcare provider may not possess information to develop a proper trust model nor can s/he enforce device-level access control in a third- party cloud health infrastructure.

5 CONCLUSION

In summary, we are envisioning a new wave of emerging health care paradigm, which is already at an early stage of inception, sweeping across healthcare services globally. This flexible patient-centered healthcare delivery system lifts the constraints of time and location of patients. Essential features of this paradigm include: (1) constant health status monitoring and intervention, (2) integrated care, (3) self- care, and (4) social support. With the advent of new information, communication, and medical technologies, the infrastructures and tool supports are already here to realize this new paradigm.

Security and privacy have already been of significant concerns in today's healthcare domain. This new paradigm, which increases the use of new and emerging technologies, hinges on even lot more collection, sharing, storage, and retrieval of health and personal information of patients. It also draws largely on more active collaboration and interactions among technological, organizational, and human entities. We delineate the security-privacy issues that surface in this anytime, anywhere health paradigm and highlights the challenges for cross-country data protection and the balance to be achieved for privacy rights.

In exploring the attack space against which anytime, anywhere healthcare paradigm must defend itself, we identify four categories: user plane, application plane, communication plane, and device plane. We survey existing approaches that can contribute to addressing the relevant privacy-security issues and identify unique challenges that existing approaches face in this new healthcare paradigm.

In broad terms, privacy and security are multi-faceted problems and require multidisciplinary approaches. Current research on privacy-security issues for data exchanges via new technologies are limited and challenging as we must realize that the problem in healthcare domain is more complex than most other domains, including e-business and manufacturing. The future directions of healthcare security-privacy research should focus efforts on mitigating these challenges. A consolidated effort from technological, human factor, and social research communities can lead to an adequate response to key privacy- security issues in this nascent anytime, anywhere healthcare paradigm.

NOTES & REFERENCES

1. Whole System Demonstrator Programme. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215264/dh_131689.pdf (accessed on June 10, 2015).

2. Katz S, Downs TD, Cash HR, Grotz RC. Progress in development of the index of ADL. Gerontologist 1970 Spring; 10(1):20-30.

3. Enthoven AC. Integrated delivery systems: the cure for fragmentation. Am J Manag Care 2009 Dec;15(10 Suppl):S284-90.

4. Nationwide Health Information Network Exchange. Available from: https://www.healthit.gov/sites/default/files/pdf/fact-sheets/nationwide-health-information-network-exchange.pdf (accessed on May 15, 2015).

5. McGowan P. "Self care behavior," in *Encyclopedia of Public Health*, L. Breslo, (ed.) Macmillan Reference USA, 2002.

6. Kaelber DC, Jha AK, Johnston D, Middleton B, Bates DW. A Research Agenda for Personal Health Records (PHRs). J Am Med Inform Assoc 2008 Nov-Dec;15(6):729-36.

7. Lorig K, Ritter PL, Laurent DD, Plant K, Green M, Jernigan VB, Case S. Online diabetes self-management program: a randomized study. Diabetes Care 2010 Jun;33(6):1275-81.

8. Medical Library Association. Health Information Literacy. Available from: https://www.mlanet.org/resources/healthlit/index.html (accessed on May 15, 2015).

9. Harvard Health. Available from: http://www.health.harvard.edu (accessed on May 15, 2015).

10. Helpguide.org [Internet]. Available from: http://helpguide.org (accessed on July10, 2015).

11. Run Keeper. Available from: http://runkeeper.com/running-app (accessed on July 10, 2015).

12. Power D. What is Social Media? Available from: http://dssresources.com/faq/index.php?action=artikel&id=226 (accessed on June 10, 2015).

13. BodySpace. http://bodyspace.bodybuilding.com (accessed on June 10, 2015).

14. Twitter Inc. http://twitter.com/

15. Domingo M. Managing healthcare through social networks. *IEEE Computer* 2010 July; 43(7):20 – 25.

16. Fat Secret. Available from: http://fatsecret.com/ (accessed on June 10, 2015).

17. Scottie – Pilot Healthcare Project. Available from: https://waag.org/en/project/pilot-healthcare-gate (accessed on May 15, 2015).

18. Office of the press secy. Remarks by the president on medical privacy. Press Release: The white house, December 2000.

19. Berendt B, Günther O, Spiekermann S. Privacy in e-commerce: stated preferences vs. actual behavior. Communication of the ACM 2005 Apr; 48(4):101–106.

20. Pew Internet and American Life Project.
Available from: http://www.pewinternet.org/2011/02/01/health-topics-4/ (accessed on May 15, 2015).

21. Poulsen K. Hackers assault epilepsy patients via computer. WIRED News 2008.

www.wired.com/politics/security/news/2008/03/epilepsy

22. Thrum S, Kane Y. Your apps are watching you. *Wall Street Journal Online*, December 2010.

23. Google Privacy & Terms. http://www.google.com/policies/privacy/partners/ (accessed on June 10, 2015).

24. Ongtang M, McLaughlin S, Enck W, McDaniel P. Semantically rich application-centric security in android. Proceedings of *2009 Annual Computer Security Applications Conference*. IEEE, 2009, pp. 340–349.

25. Cheng Z. Mobile malware: Threats and preventions. McAfee Avert Lab, Tech. Rep., sep 2007.

26. Au K, Zhou Y, Huang Z, Gill P, Lie D. Short paper: a look at smartphone permission models. *Proceedings of the1st ACM workshop on Security and privacy in smartphones and mobile devices*, ser. SPSM '11. New York, NY, USA: ACM, 2011, pp. 63–68.

27. Henry A. Facebook Is Tracking Your Every Move on the Web; Here's How to Stop It. LIFEHACKER 2011 Sept. 26. Available from: http://lifehacker.com/5843969/facebook-is-tracking-your- every-move-on-the-web-heres-how-to-stop-it

28. Omre AH, Keeping S. Bluetooth low energy: Wireless connectivity for medical monitoring. J. Diabetes Sci. Technol 2010; 4(2): 457–463.

29. Mare S, Kotz D. Is Bluetooth the right technology for mhealth? Proceedings of USENIX Workshop on Health Security and Privacy (HealthSec). August, 2010.

30. Li C, Raghunathan A, Jha N. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. in *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, June 2011, pp. 150 –156.

31. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: *2008 IEEE Symposium on Security and Privacy*. IEEE, 2008, pp. 129–142.

32. Ashar BS, Ferriter A. Radiofrequency identification technology in health care: benefits and potential risks. *JAMA* 2007 Nov 21; 298(19):2305-7.

33. MANAGED CARE, 2014 Aug, Available from: http://www.managedcaremag.com/archives/2014/8/medical-device-market-hit-133-billion-2016 (accessed on June 10, 2015).

34. Stanton J, Stam K, Mastrangelo P, Jolton J. Analysis of end user security behaviors. *Computers Security* 2005; 24(2):124–133.

35. Gollakota S, Hassanieh H, Ransford B, Katabi D, Fu K. They can hear your heartbeats: non-invasive security for implantable medical devices. *SIGCOMM Computer Communication Review* 2011 Aug; 41(4): 2–13.

36. Yang Y, Lewis E, Brown L. Cultural and social aspects of security and privacy: the critical elements of trusted online service. In: *Proceedings of the 2nd international conference on Usability and internationalization*, ser. UI-HCII'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 546–553.

37. Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges. OCED 30 May 2013 Accessed April 19, 2015 via http://www.oecd.org/els/health-systems/strengthening-health-information-infrastructure.htm

38. Arkin B, Stender S, McGraw G. Software penetration testing. *IEEE Security & Privacy* 2005 Jan-Feb; 3(1):84–87.

39. Nico PL, Turner CS, Nico KK. Insecurity by contract. In: *Proceedings of the 8th IASTED International Conference on Software Engineering and Applications (SEA 2004)*, November 2004, pp. 269–274.

40. Saltzer J, Schroeder M. The protection of information in computer systems. In: *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sept. 1975.

41. Davi L, Dmitrienko A, Sadeghi AR, Winandy M. Privilege escalation attacks on android. In: *Proceedings of Information Security*, ser. Lecture Notes in Computer Science, M. Burmester, G. Tsudik, S. Magliveras, and I. Ilic, (eds.) Springer Berlin / Heidelberg, 2011, vol. 6531, pp. 346–360.

42. Motiee S, Hawkey K, Beznosov K. Do windows users follow the principle of least privilege?: investigating user account control practices. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10. New York, NY, USA: ACM, 2010, pp. 1:1–1:13.

43. Ardagna CA, di Vimercati SDC, Foresti S, Grandison TW, Jajodia S, Samarati P. Access control for smarter healthcare using policy spaces. Computers and Security. 2010;29(8):848 – 858.

44. Aggarwal CC. On k-anonymity and the curse of dimensionality. In: *Proceedings of the 31st International Conference on Very Large Data Bases,* ser. VLDB '05. VLDB Endowment, 2005, pp. 901–909.

45. Oganian A, Domingo-Ferrer J. On the complexity of optimal micro-aggregation for statistical disclosure control. Statistical Journal of the United Nations Economic Commission for Europe. 2001;18(4):345–353.

46. Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: Ensuring privacy of electronic medical records. In: *The ACM Cloud Computing Security Workshop (CCSW'09)*. ACM, 2009.

47. Ibraimi L, Asim M, Petkovic M. Secure management of personal health records by applying attribute-based encryption. In: *Wearable Micro and NanoTechnologies for Personalized Health (pHealth), 2009 6th International Workshop on*, June 2009, pp. 71–74.

48. Narayan S, Gagné M, Safavi-Naini, R. Privacy preserving EHR system using attribute-based infrastructure. In: *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, ser. CCSW '10. New York, NY, USA: ACM, 2010, pp. 47–52.

49. Akinyele JA, Pagano MW, Green MD, Lehmann CU, Peterson ZN, Rubin AD. Securing electronic medical records using attribute-based encryption on mobile devices. In: *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, ser. SPSM '11. New York, NY, USA: ACM, 2011, pp. 75–86.

50. Dhamija R, Tygar JD, Hearst M. Why phishing works. In: *Proceedings of the SIGCHI conference on Human Factors in computing systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 581–590.

51. Kumaraguru P, Sheng S, Acquisti A, Cranor LF, Hong J. Lessons from a real world evaluation of anti-phishing training. In: *IEEE eCrime Researchers Summit*, 2008, pp. 1–12.

52. Gorling S. The myth of user education. In: Proceedings of the 16th Virus Bulletin Int. Conference, 2006.

53. Park S, Matthews B, D'Amours D, McIver Jr. WJ. Characterizing the impacts of VPN security models on streaming video. In: *Proceedings of the 2010 8th Annual Communication Networks and Services Research Conference*, ser. CNSR '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 152–159.

54. Shieh YY, Tsai FY, Wang MD, Lin CM. Mobile health care: Opportunities and challenges. In: *International Conference on the Management of Mobile Business (ICMB '07)*, July 2007.

55. Giani A, Roosta T, Sastry S. Integrity checker for wireless sensor networks in health care applications. In: *Second International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '08)*, Feb. 2008, pp. 135 – 138.

56. Arazi B. Message authentication in computationally constrained environments. *IEEE Transactions on Mobile Computing* 2009 july;8(7):968 –974.

57. Rosales MS, Garcia GG, Sanchez GD. Efficient message authentication protocol for WSN. *WSEAS Transactions on Computers* 2009 June;8(6):895–904.

58. Xu F, Qin Z, Tan C, Wang B, Li Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In: *IEEE Proceedings of INFOCOM*, April 2011, pp. 1862 – 1870.

59. Schechter S. Security that is meant to be skindeep using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. In: *First USENIX Workshop on Health Security and Privacy (HealthSec)*, 2010.

60. Cherukuri S, Venkatasubramanian K, & S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," In: *Proceedings of the International Conference on Parallel Processing Workshops*, Oct. 2003, pp. 432 – 439.

61. Denning T, Fu K, Kohno T. Absence makes the heart grow fonder: new directions for implantable medical device security. In: *Proceedings of the 3rd conference on Hot topics in security*. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–7.

62. Rae A, Fidge C. Information flow analysis for fail-secure devices. *The Computer Journal* 2005 Jan; 48(1):17–26.

63. Bussard L, Roudier Y, Kilian-kehr R, Crosta S. Trust and authorization in pervasive b2e scenarios. In: *The Fifth International Conference on Ubiquitous Computing (UbiComp)*, Springer, 2003.

64. Wicks P, Massagli M, Frost J, Brownstein C, Okun S, Vaughan T, Bradley R, Heywood J. Sharing health data for better outcomes on PatientsLikeMe. *J Med Internet Res*. 2010 Jun 14;12(2):e19.

65. MyOSCAR. Available from: http://myoscar.org (accessed on July 12, 2015)

66. Novant Health MyChart. Available from: https://novantmychart.org/ (accessed on July 12, 2015)

67. NextGen Healthcare Patient Portal. Available from: https://www.nextmd.com/ (accessed on July 12, 2015).

68. HealthVault. Available from: https://www.healthvault.com/ (accessed on July 12, 2015).

69. Ackerman MS, Cranor LF, Reagle J. Privacy in e-commerce: Examining user scenarios and privacy preferences. In: *Proceedings of the ACM Conference on Electronic Commerce EC'99,* Denver, CO: Nov.1999, pp. 1-8

70. U.S. Food and Drug Administration. Medical Device Recall Report. Available from: http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/UCM388442.pdf (accessed on June 10, 2015).