Smart Homecare Technology and TeleHealth

Dovepress
open access to scientific and medical research

Open Access Full Text Article

ORIGINAL RESEARCH

Health care professionals' perception of security of personal health devices

This article was published in the following Dove Press journal:
Smart Homecare Technology and TeleHealth
12 April 2017
Number of times this article has been viewed

Brian Ondiege
Malcolm Clarke

Department of Computer Science, College of Engineering, Design and Physical Sciences, Brunel University London, UK

Abstract: With the rapid advances in the capabilities of telehealth devices and their increasing connection to the Internet, security is becoming an issue of major concern. Therefore, the perceptions of the health care professionals regarding security are of interest, as the patients trust them to make informed decisions on issues concerning their privacy, data, and health. Eight health care professionals were interviewed to determine their perceptions and knowledge of security in health care. The research further examines one specific aspect of security which is considered of significant concern: the authenticity of a device being from the actual manufacturer and not a counterfeit. This research proposes device registration together with digital signatures and one-time passwords to address the issue of counterfeit remote patient-monitoring devices and identify and authenticate the user of the device.

Keywords: telehealth security, health care professionals' perception, personal health device, authentication

Introduction

Perception is the subjective human understanding of a topic and will determine how an individual will respond to a specific issue. Understanding perception is critical to understanding and determining the behavior of an individual and can be used to predict how he/she might interact with a system.[1]

Security is becoming a sensitive topic, especially with recent advances in the technology used in telehealth. Patients trust health care professionals to maintain their privacy, confidentiality, and health; therefore, it is important to have mechanisms in place that can protect the privacy of a patient.[2] However, such mechanisms generally need to be proactive on behalf of the organization and users who care for the data. Therefore, this research investigates the perception of health care professionals toward security and their knowledge of the threats in information security. It further investigates one approach to address the issue of counterfeit remote patient-monitoring (RPM) devices.

This study was undertaken in selected hospitals and a health care center in London, UK, which are actively practicing telehealth.

Information security may be considered to have three main aspects:

- confidentiality – which is the prevention of unlawful revelation of information;
- integrity – which is the prevention of unlawful alteration of information; and
- availability – which is the prevention of unlawful withholding of information or resources.[3]

Correspondence: Brian Ondiege
Department of Computer Science, St John's Building, Brunel University London, St John's Building, Kingston Lane, Uxbridge, Middlesex, London UB8 3PH, UK
Tel +44 75 4288 7874
Email brian.ondiege@brunel.ac.uk

Terminologies

- Information security in health care sector – protection of personal health-related devices and records from any unauthorized access, modification, disclosure, or use.[4]
- Medical identity theft – the illegal access and use of personally identifiable information to obtain medical service, prescription drugs, or medical insurance coverage by fraud. It includes medical insurance numbers, medical care numbers, or patient or physician identification numbers that may be used directly or sold on the black market.[5] Stolen medical identities are most frequently used to obtain addictive prescription medications.
- Personal health device (PHD) – a device used directly by the patient to obtain clinical observations. This includes devices such as weighing scales, blood pressure monitors, and blood glucose monitors.

Objectives of the research

The term health care professional has been used in this study to describe doctors and nurses. Counterfeit can be defined as made in exact imitation or forgery with intent to deceive or defraud.

The objectives of this study were to determine the perception of health care professionals on information security and to address the issue of counterfeit RPM devices to include the following:

- What is the level of perception held by health care professionals?
- What factors influence the perception of health care professionals?
- What is the level of awareness of health care professionals of security in their working environment?
- What are the implications of a breach of security, and how would it affect the health care professionals and their patients?
- What are the risks involved in the misidentification of patients in RPM?
- What are the appropriate identification techniques for frail elderly using PHDs?
- How can devices be authenticated to ensure genuine manufacture and not counterfeit?

Research significance

Although security in health care is a popular topic for research, no articles have been published on the perception and knowledge of health care professionals on information security in the health care environment, despite security being paramount for managing personal information.

Telehealth has probably suffered as security does always receive the attention that is required during the development stages of a technology, and this deficiency could leave telehealth vulnerable to malicious attacks. The problems include patient identification, incorrect readings, and counterfeit (inaccurate) devices, each of which can put the life of a patient at risk.[6]

Telehealth research shows that one of the main gaps in RPM architecture research is that the issue of security is not considered because the researchers are not familiar with it.[7] These findings suggest that telehealth and RPM devices could provide a perfect playing field for opportunistic security attacks. In addition, the current RPM devices are limited in terms of the number of users who can use each device at a given time, and only the person who is being monitored is allowed to use the device.[8,9]

The problem of patient identification relates to the ability to verify the person using the device is the actual patient. Problems frequently arise from visitors inadvertently using the device and causing incorrect data to be recorded. In addition, patients may persuade others to take a reading on their behalf.

Incorrect readings arise from a patient not following a prescribed protocol. This can include the following: not taking measurements at the same time of the day; repeatedly taking a measurement; taking measurements under different circumstances, such as wearing different amounts of clothing when taking a weight; not taking sufficient care during a measurement, such as holding a pet; and incorrect procedure.

Counterfeit medical devices pose a threat as they are often not manufactured to the required standard of accuracy as the original device and their use will result in inaccurate readings.

Research has identified cases where misidentification of a device has led to the device not being recognized and putting the health of the patient at risk.[10] For example, it took 2 weeks to find 30 patients affected by a recent recall of patients following a hip replacement. The problem is often exacerbated by manufacturers using different coding schemes to identify products and their unique serial number, making it difficult to trace device to patient.[10]

In health care, diseases such as diabetes rely on accurate measurements for treatment; if a device is lost or is replaced with a rogue or compromised device and then introduced into the ecosystem, there are high chances of it sending the wrong reading, which will trigger the wrong treatment that might endanger the patients' life.[11]

Research methodology

Design of the study

Semi-structured interviews were used in this research to elicit the perceptions of the health care professionals toward information security and security issues in telehealth. Ten questions were prepared in advance for a direct conversion on the two most salient topics of the study: security in general and security of RPM devices.

The rationale for using a qualitative approach in this study was to explore and describe the opinion of health care professionals' general perception of security. A qualitative approach was appropriate to capture the opinions of health care professionals regarding security.

This is a descriptive research as it looks the general perception of health care professionals on security with a view to improve security practices and awareness.

Study area

The study was conducted in four London health care settings, including three hospitals (Ealing Hospital, Royal Free Hospital, and Hillingdon Hospital) and one health care center (Chorleywood Health Centre). Eight health care professionals were interviewed over the period from January 2014 to February 2014.

Sampling techniques and sample size

Participants were included from health care organizations that were practicing telehealth and those identified as being actively engaged in telehealth. Interviews were conducted with the health care professionals in their respective organization.

Ethics and consent

The study received ethical approval from Brunel University Ethics Committee. The objective of the research was explained to each participant, and informed consent was obtained prior to starting the interview.

Data collection instrument and method

All interviews were digitally recorded and later transcribed. Thematic analysis was used on the data in order to identify the important themes and to understand the significance of the themes identified in advance from the literature survey.

Results

Demographics

Table 1 provides the demographics of the participants of the study. The data include gender and the number of participants.

Table 1 Demographics

Age (years)	Gender	Participants
18–30	M	1
	F	2
31–45	M	1
	F	3
>45	M	1
	F	0
Total		8

Abbreviations: M, male; F, female.

Responses

Question 1 – access to email and Internet

Question 1 was related to access to email and the Internet. All the participants confirmed that they had an email account. However, the frequency and the length of time spent on the Internet varied. Age was a major factor. Participants aged <40 years accessed the Internet more often and used social networks. Respondents aged >40 years used the Internet less often, with two of them using it for only work purposes. Two used it for both work and personal use.

Question 2 – email intrusion

Question 2 asked whether the participants had ever had their email account compromised by a hacker. The aim of this question was to determine whether they had encountered a security issue and whether they were aware of its nature. Six participants believed that they had had their accounts compromised by hackers, either their account had become inaccessible or they were told their passwords were changed.

Question 3 – passwords

Question 3 investigated perception of passwords. The aim of this question was to determine whether the participants were aware that passwords can be guessed or discovered by brute force and of the dangers of having passwords that are easily guessed. Three of the participants believed their passwords to be secure. Five commented that they had a problem to remember passwords, especially if they were told to change their passwords often. One nurse informed that she had used "password" as her password.

Question 4 – computer virus

Question 4 asked about computer viruses. Only one doctor and one nurse correctly described a computer virus as a malicious program. The remainder of the participants were unaware of what a computer virus was.

Question 5 – security of passwords

Question 5 asked further about the perception of the security of passwords. Four participants believed passwords to be

secure, two responded that they could be insecure, and two answered that they did not know. A follow-up question asked about the significance of having a password with many characters. Two answered that it gave protection against hackers, but six answered that they did not know the reason.

Question 6 – information security

Question 6 investigated the level of knowledge of the participants regarding the nature of information security. Two participants indicated that they had some knowledge of information security, but six of the participants admitted to having little or no knowledge.

Question 7 – security of storage systems

Question 7 investigated the level of trust that each participant had in his/her current system for storing health records. All the participants believed that their system was secure. A follow-up question asked how they knew that it was secure. All the participants responded that they had been informed by the National Health Service that it was secure but had been given no information on the details of how it was secure.

Question 8 – security of patient records

Question 8 related to the security of the storage of patient records. Four doctors said they were unaware of the location of patient records as the nurses brought the records to them whenever a patient was visiting the hospital. Four nurses described how some records were stored online in a database but paper records were stored in the hospital. A follow-up question asked about the access control mechanisms to the records. The nurses responded that "the only form of access control is lock and key so nurses and cleaners have access to the storage area of the records."

Question 9 – RPM

Question 9 was related to the security of RPM devices. The aim of this question was to determine the security of the devices and the dangers that can be associated with misidentification of patients. The participants were asked how they knew the identity of person sending observations. All the participants explained that each device has a unique identifier that is used to identify the patient who is using the device. A follow-up question asked how they could verify the identity of the person using the device. All the respondents replied that they could not know because the devices had no means of identification or authentication of a patient.

Question 10 – device authentication

Question 10 investigated device authentication and how it may be determined if a RPM device was genuine or counterfeit. None of the respondents could answer this question. All the participants were aware of counterfeit products, but were unaware how to recognize a counterfeit device. One doctor answered, "If it's packaged like the original one and looks like an original one how would one know?"

It was pointed out that the problem of device authentication is not limited to telehealth but affects the entire health care industry.

Device authentication and patient verification

This study has identified specific security issues that need to be resolved if they are not to be a threat to the implementation of telehealth. This includes counterfeit RPM devices and the identification and verification of the actual patient making observations. One-time passwords (OTPs) and digital signatures are proposed and investigated as a solution for device authentication. The proposed model is tested to evaluate its effectiveness and usability.

This study examines ISO/IEEE 11073 which is a standard for PHD and addresses security and authentication of telehealth devices which is critical in determining the integrity of a telehealth system.

Device registration with OTPs and digital signatures

OTPs

An OTP is defined as a password that has validity for one session only. Each new session requires that a new OTP is obtained. OTPs have the advantage that they cannot be attacked by guessing or brute force, can be created to be random and of sufficient length to be secure, and are not physically open to access. Access implementation with OTP may also incorporate authentication by a secret known only to the person.[12]

Digital signature

A digital signature can be defined as a mathematical scheme that is capable of demonstrating authentication, integrity, and non-repudiation of a message. The validity of a digital signature provides proof to the recipient that a received message was created by the disclosed sender (authentication), the sender cannot deny having sent the message (non-repudiation), and that the received message was not altered in transit.[13]

Device registration

When a patient first receives an RPM device, he/she registers it with a service by providing the identification details and the unique product identifier of the device. During the registration process, a challenge response OTP authentication code is sent to the patient by using a validated message address, such as email. Each authentication code is tamper-proof and cannot be forged. On receiving the token, the patient can make a request to determine if the device is genuine.

A simulation of the environment is created and tested. Figure 1 shows the proposed framework model and the information flow between a patient-monitoring device and the service.

When the patient receives the authentication code, this means he/she is ready to register the device status. In the simulation, the user is asked to log in via a secure web browser. The patient enters his/her registration details and registers the device. To be authenticated (1), the patient submits the same username to the authentication server as used during log in (2). The authentication server responds by issuing a challenge which is an authentication code sent to his/her email address (3). The patient retrieves the email with the OTP and then sends the OTP, date and time requested, and previous attributes signed with the private key of the patient as response (4). The authentication server checks the response of the OTP (5), and if successful, will submit the request ID, message, date and time, hash, username, and signature to the registration server (6). The registration server will check the OTP and also compare the hash value with the signature (7). If the OTP, the hash value, and the signature match, the registration server will respond by authenticating the device. If not, the registration server will issue a message that the device is not valid. If a device is authenticated, details about the device (eg, manufactured date, name of the device) will be displayed, and an audit log containing the request and the digital signature will be submitted to the request log.

For each request, a secure hash (SHA-1) is generated against the attributes (date and time, request ID, username, and request message) and then digitally signed. Sending the request attributes and its digital signature will further ensure that the request cannot be altered.

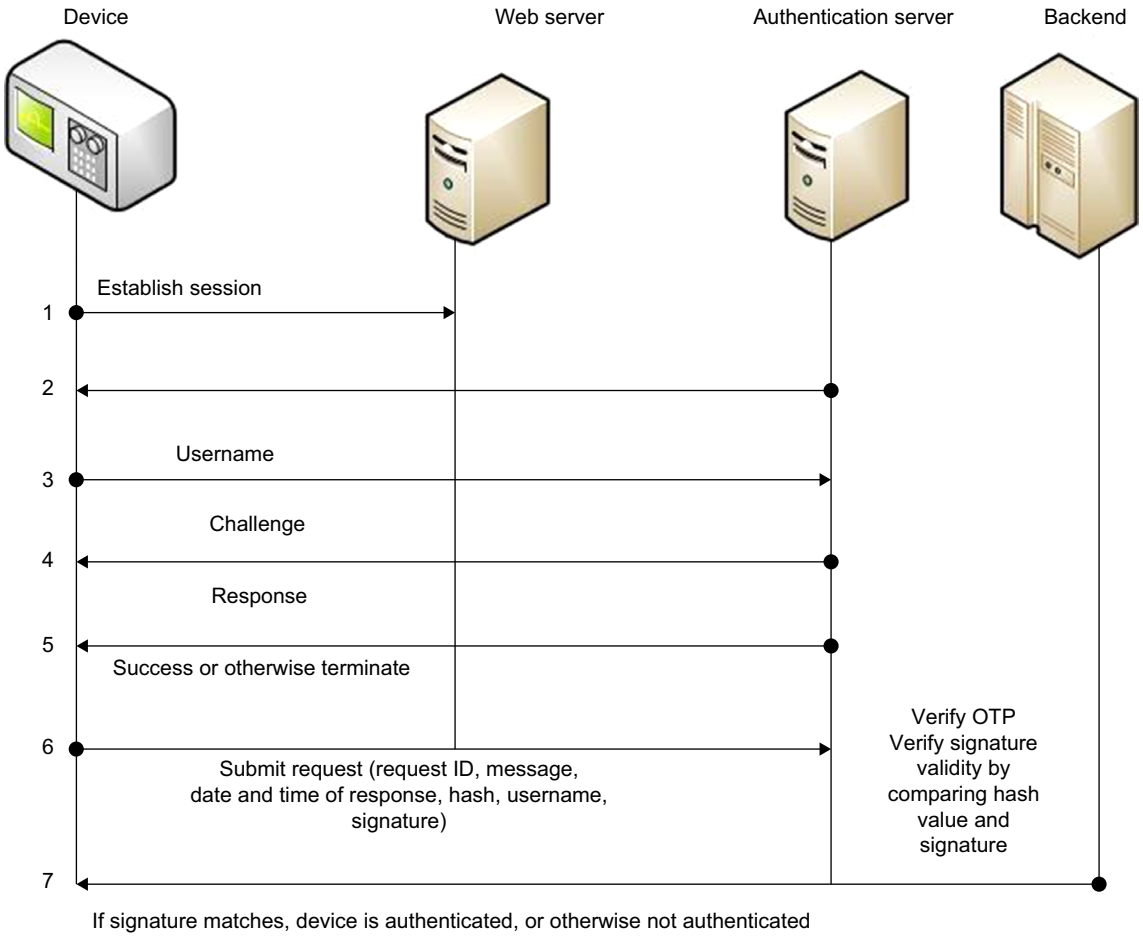

Figure 1 Device authentication using OTP and digital signatures.
Abbreviation: OTP, one-time password.

If there is a dispute over the authenticity of a request, this can be resolved by examination of the signed confirmation using the public key of the patient. Figure 2 shows a log of signed information that could be used to resolve a case of repudiation for a registered and authenticated device.

Users mailbox

The OTP is randomly generated and can be used only once during authentication. The users log into the mailbox that they used during registration to retrieve the OTP that was sent to them. The OTP is used in the process of RPM authentication.

Patient identification

Lack of a proper identification technique in PHDs can lead to verification problems. If a patient cannot be properly verified, he/she may not receive correct care, or worse, may receive incorrect care.

This study recognizes the importance of having a proper identification. However, telehealth technology should be easy to use, as it is used extensively by the frail elderly. Any solution should be designed for the frail elderly, but also needs to remain cost-effective.

Many conflicting factors need to be considered in selecting an identification technique that can be used by the frail elderly on PHDs.

Near-field communication (NFC) technology is proposed as a solution to the problem of identification of a patient using a PHD. Presentation of a card, or similar, to the device in advance of a measurement can validate and identify the user. Work is being undertaken to evaluate the approach by modifying a blood pressure monitor to incorporate identification and verification by using NFC technology.

Why NFC technology?

NFC is a set of communication protocols that allow two electronic devices, one of which is usually a portable device such as a smartphone, to start communication by bringing them within 4 cm of each other.

The following criteria were used in selecting NFC.[14]

Usability

Usability plays a vital role in technology for old people; it builds confidence and trust when using technology.

Patients should not have to think too hard when they are using a technology, nor should they have to refer to a manual when using it; this makes them look less intelligent and leads to time wastage.

Device prompts should be logical, sequential, and effortless to ensure that the patient uses less time, enjoys using the device, makes a recommendation, and looks forward to using it continuously. NFC technology provides an effortless and fast means of identification and authentication.

Familiarity

NFC technology is widely used in Great Britain and other developed countries. In London, people are using it for public transport as part of the Transport for London network and in making payments at the grocery stores. This study identified that NFC technology will elicit different reactions, with most of them being positive due to ease of use and very few negatives for those who are not familiar with the technology.

Cost

Cost plays a vital role in implementation of any technology. NFC technology is affordable and secure; an NFC card costs <40 p and can be reused multiple times by different users, which makes it economically viable.

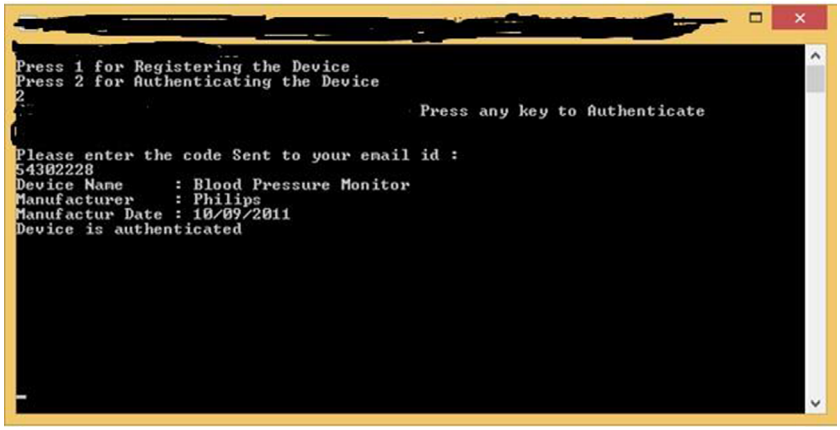

Figure 2 Device authentication.

Identification with NFC alone is not sufficient; therefore, there is a need for a solution that will increase the security within the NFC framework. This study proposes the use of a capability-based system because NFC_ID can be tampered while in storage or while in use.[15] It provides additional security by restricting access to data, people, and devices.

Capabilities are therefore especially applicable in the context of eHealth as health data are very sensitive and hence must be protected from tampering and unauthorized access. Furthermore, capabilities allow us to run a role-based mechanism, so restrictions can be based on the role of different people within the health care system such as doctors, nurses, technicians, and administrators. Therefore, in this system, each entity must have a capability; for example, people, devices, and infrastructure all must have capabilities. Capabilities can also be used to provide restrictions to access to data and resources to personnel based on their roles. Figure 3 presents the new format that will be used to present capabilities. More details on this capability format are found in the study by Mapp et al.[15]

- Type field: This field is used to specify the type of object capability that is being used. Types could include Cloud providers, Cloud platforms, users, and applications.
- Property field: This field is used to define the properties of the object.
- Object ID: This field is used to uniquely identify the object.
- Random bit field: This field helps to uniquely identify the object.
- Hash field: This field is used to prevent the casual tampering of capabilities.

To enhance patients' privacy, this study proposes the use of user authentication schemes for the protection of patients' privacy and prevention of common security attacks.[16,17]

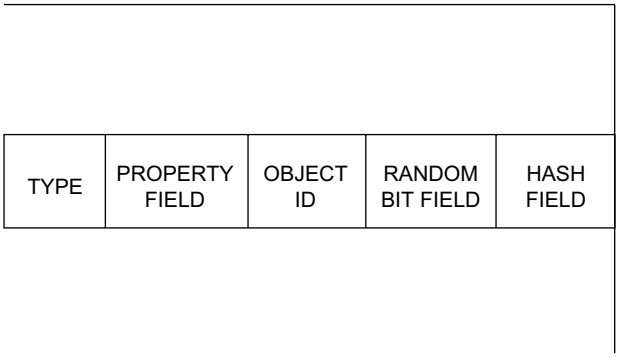

Figure 3 New capability format
Notes: When an object capability is created the type, properties, and object Id fields are first generated. The random parts are then generated. Finally, these fields are used to generate a SHA-1 hash which is placed in the hash field of the capability.

Conclusion

The aim of this study was to determine the level of perception and knowledge of security among health care professionals. The outcome of this study indicates that the perception of health care professionals toward the importance of security is very low and their knowledge about security issues is poor. Such poor awareness of security among the users poses significant danger for the integrity of health care systems. This is especially important while adopting new technologies before all the threats are recognized and mitigated. Telehealth, still being in its early stages of development, leaves it vulnerable to security attacks. Such threats in security could undermine confidence in its full implementation, and so it is very important that health care professionals are made aware of the security issues.

This study further identified specific threats to the implementation of telehealth. These include counterfeit RPM devices and the identification and verification of the actual patient making observations. Digital signatures and OTPs were proposed and investigated as a solution for device authentication and certify that the devices are genuine. Each device is bound to the patient who registered the device, and so the hospital can ensure that the devices are registered – any counterfeit device will not be authenticated and therefore will not be allowed to be used.

The study highlights the importance of patient identification in home monitoring devices. The World Health Organization states that failure to correctly identify patients can result in wrong diagnosis, transfusion errors, and testing errors. The US is trying to make patient identification one of its patient safety goals and so reduce errors caused by patient misidentification.[18]

There are a limited number of health care professionals actively engaged in telehealth in the locality and available for interview. Furthermore, a significant number of those approached declined to participate in the study. These limitations resulted in only eight participants agreeing to participate.

The approaches and results of this research can be used in the evaluation of security practices in the health care setting, and proposing best security practices in health care. This research recommends creating awareness workshops that can be used to educate clinicians about the importance of security in the health care setting. Moreover, health care professionals need to be trained on security standards 95/46 EC and ISO 27002 that emphasize security practices and the importance of enforcing these standards within their practices.[19,20]

Disclosure

The authors report no conflicts of interest in this work.

References

1. Huang DL, Rau P-LP, Salvendy G, Gao F, Zhou J. Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int J Hum Comput Stud*. 2011;69(12):870–883.
2. Marianne Kolbasuk McGee. (2012). A Patient Data Matching Call to Action. Available from: http://www.healthcareinfosecurity.com/interviews/patient-data-matching-call-to-action-i-1673. Accessed May 2, 2014.
3. Ferreira A, Antunes L, Chadwicka D, Correia R. Grounding information security in healthcare. *Int J Med Inform*. 2010;79(4):268–283.
4. Tesema T, Medlin D, Abraham A. Patient's perception of health information security: the case of selected public and private hospitals in Addis Ababa. Paper presented at: Sixth International Conference of Information Assurance and Security (IAS); Atlanta, GA, USA: 23–25 Aug, 2010.
5. Techtarget medical identity theft. Available from: http://whatis.techtarget.com/definition/medical-identity-theft. Accessed March 20, 2016.
6. Natarajan S, Wottawa CR, Dutson EP. Minimization of patient misidentification through proximity-based medical record retrieval. In: ICME International Conference on Complex Medical Engineering; Tempe, AZ, USA: April 9–11, 2009.
7. Garg V, Brewer J. Telemedicine security: a systemic review. *J Diabetes Sci Technol*. 2011;5(3):768–777.
8. Continua Health Alliance. Recommendations for proper user identification in Continua version 1—PAN and xHR interfaces. 2008. Available from: https://cw.continuaalliance.org/document/dl/download/3734. Accessed July 8, 2016.
9. Ondiege B, Clarke M. Healthcare professionals perception on information security: IADIS. In: Proceedings of the 5th International Conference on Internet Technologies and Society; December 10–12, 2014; Taipei.
10. GS1 Healthcare White Paper on UDI implementation. Global standards pave the way for unique device identification (UDI). 2011. Available from: www.gs1.org/docs/healthcare/GS1_UDI_Position_Paper.pdf. Accessed May 4, 2016.
11. Petković M. Remote patient monitoring: information reliability challenges. In: 9th International Conference on Telecommunication in Modern Satellite, Cable, and Broadcasting Services; Niš, Serbia: October 7–9, 2009.
12. Defuse. Encrypting One Time Passwords. Available from: https://defuse.ca/eotp.htm. Accessed August 29, 2015.
13. Martiri E, Baxhaku A. Monotone digital signatures: an application in software copy protection. *Procedia Technol*. 2012;1:275–279.
14. Ondiege B, Clarke M, Mapp GE. Exploring security of remote patient monitoring devices using NFC technology for identification of the frail elderly. In: 8th International Conference of e-Health, IADIS; July 1–3, 2016; Funchal.
15. Mapp G, Aiash M, Ondiege B, Clarke M. Exploring a new security framework for Cloud storage using capabilities. In: 1st International Workshop on Cyber Security and Cloud Computing; April 7–11, 2014; Oxford.
16. Amin R, Biswas GP. An improved RSA based user authentication and session key agreement protocol usable in TMIS. *J Med Syst*. 2015;39(8):79.
17. Mir O, van der Weide T, Lee C-C. A secure user anonymity and authentication scheme using AVISPA for Telecare medical information systems. *J Med Syst*. 2015;39(9):89.
18. WHO Impact Evaluation. Patient identification policy. 2011. Available from: http://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf. Accessed March 4, 2015.
19. Introduction to ISO 27002 (ISO27002). Available from: www.27000.org/iso-27002.htm. Accessed March 20, 2015.
20. EU Directive 95/46/EC – The Data Protection Directive. Chapter 2 – General rules on the lawfulness of the processing of personal data. Available from: https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm. Accessed September 4, 2014.