Healthcare professionals' perception of security of Personal Health Devices

Brian Ondiege
School of Information Science, Computing and Mathematics, Brunel University
Kingston Lane, Uxbridge, London
Brian.ondiege@brunel.ac.uk

Malcolm Clarke
School of Information Science, Computing and Mathematics, Brunel University
Kingston Lane, Uxbridge, London
Malcolm.clarke@brunel.ac.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 healthcare professional regarding security are of interest, as the patients trust them to make informed decisions on issues concerning their privacy, data and health. Eight healthcare professionals were interviewed to determine their perceptions and knowledge of security in healthcare. The research further examines one specific aspect of security which was 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 (OTP) to address the issue of counterfeit remote patient monitoring devices and identify and authenticate the user of the device.

KEYWORDS

Telehealth Security, Healthcare professionals' perception, Personal Health Device, , Authentication,

1. 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 behaviour of an individual and can be used to predict how they might interact with a system [1]

Security is becoming a sensitive topic, especially with recent advances in the technology used in telehealth. Patients trust healthcare 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 organisation and users that care for the data. This research therefore investigates the perception of healthcare professionals towards security and their knowledge of the threats in information security. It further investigates one approach to address the issue of counterfeit remote patient monitoring devices.

This study was undertaken in selected hospitals and a health care centre in London, U.K. that are actively practicing telehealth.
Information security may be considered to have three main aspects;

1. Confidentiality – which is the prevention of unlawful revelation of information;
2. Integrity - which is the prevention of unlawful alteration of information;
3. Availability - which is the prevention of unlawful withholding of information or resources [3]

1.2 Terminologies

- Information Security in Healthcare 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, blood glucose monitors etc.

1.3 Objective of the Research

The term healthcare 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 are to determine the perception of healthcare professionals on information security and to address the issue of counterfeit remote patient monitoring devices to include:

- What is the level of perception held by healthcare professionals?
- What factors influence the perception of healthcare professionals?
- What is the level of awareness of healthcare professionals of security in their working environment?
- What are the implications of a breach of security and how would it affect them and their patients?
- What are the risks involved in the misidentification of patients in remote patient monitoring?

- What are appropriate identification techniques for frail elderly using Personal Health Devices (PHD)?
- How can devices be authenticated to ensure genuine manufacture and not counterfeit?

1.4 Research Significance

Although security in healthcare is a popular topic for research, no articles have been published on the perception and knowledge of healthcare professionals on information security in the healthcare 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.

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 that 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. Additionally, 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: not taking measurements at the same time of the day; repeatedly taking a measurement; taking measurements under different circumstance, 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 two 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 healthcare, 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].

2. RESEARCH METHODOLOGY

2.1 Design of the study

Semi-structured interviews were used in this research to elicit the perceptions of the healthcare professionals towards information security and security issues in telehealth. Ten questions were prepared in advance to direct conversion on the two most salient topics of the study; security in general and security of remote patient monitoring devices.
The rationale for using a qualitative approach in this study was to explore and describe the opinion of healthcare professionals' general perception of security. A qualitative approach was appropriate to capture the opinions of healthcare professionals regarding security.
This is descriptive research as it looks the general perception of healthcare professionals on security with a view to improve security practices and awareness.

2.2 Study area

The study was conducted in 4 London healthcare settings, including three hospitals (Ealing Hospital, Royal Free Hospital and Hillingdon Hospital) and one healthcare centre, (Chorleywood Health Centre). Eight healthcare professionals were interviewed over the period from January 2014 to February 2014.

2.3 Sampling techniques and sample size

Participants were taken from healthcare organisations that were practicing telehealth and the participant identified as being actively engaged in telehealth. Interviews were conducted with the healthcare professional in their respective organisation.

2.4 Ethics and consent

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

2.5 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.

3. Results

3.1 Demographics

Table I provides the demographics of the participants of the study. The data includes gender and the number of participants.

TTable 1 demographics		
Age	Gender	Participants
18-30	M	1
	F	2
31-45	M	1
	F	3
>45	M	1
	F	0
Total		8

3.2. Responses

Question 1 - access to email and internet

Question 1 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 under 40 years old accessed the internet more often and used social networks. Respondents over 40 years used the internet less often, with two of them only using it for work purposes. Two used it for both work and personal use.

Question 2 – email intrusion

Question 2 asked if the participants had ever had their email account compromised by a hacker. The aim of this question was to determine if they had encountered a security issue and if 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 if the participants were aware that passwords can be guessed or discovered by brute force and the dangers of having passwords that are easily guessed. Three of the participants believed them 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 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 their 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 NHS 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 – remote patient monitoring
Question 9 related to the security of remote patient monitoring 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 that 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 how it may be determined if a remote patient monitoring 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 recognise 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 healthcare industry.

4. 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 remote patient monitoring devices and the identification and verification of the actual patient making observations. One-time Passwords (OTP) 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 Personal Health Device (PHD) and addresses security and authentication of telehealth devices which is critical in determining the integrity of a telehealth system.

4.1 Device registration with OTP and digital signatures

4.1.1 OTP

A One-time Password (OTP) is defined as a password that has validity for one session only. Each new session requires that a new OTP is obtained. OTP 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 not physically open to access. Access implementation with OTP may also incorporate authentication by a secret known only to the person [12].

4.2.2 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].

4.2.3 Device Registration

When a patient first receives a remote patient monitoring device they register it with a service by providing their 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 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 was created and tested. Figure I shows the proposed framework model and the information flow between a patient monitoring device and the service.

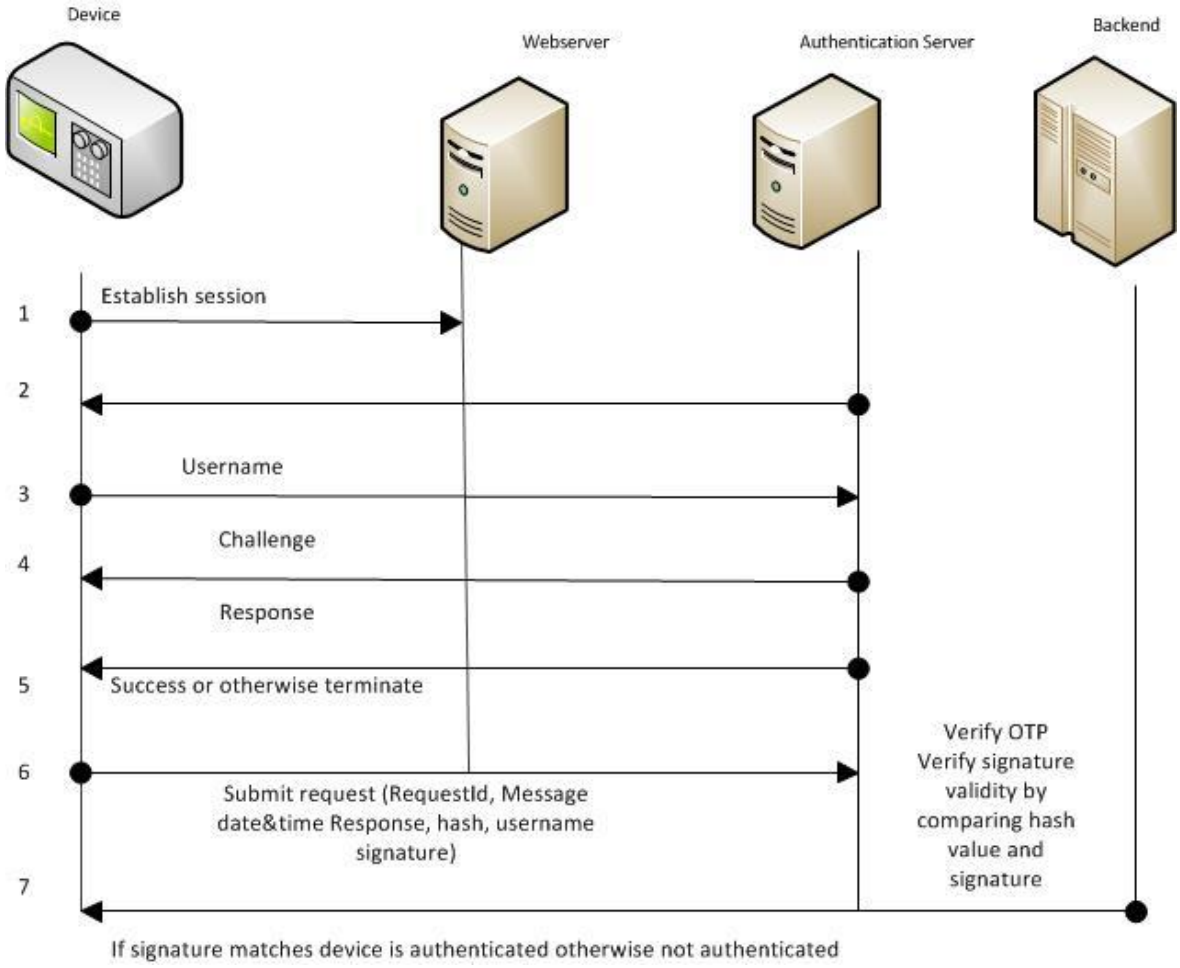

Figure I Device Authentication using OTP and digital signatures

When the patient receives the authentication code, this means they are ready to register the device status. In the simulation the user was asked to log in via a secure web browser. The patient enters their registration details and registers their 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 their 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 (e.g.

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.

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 II shows a log of signed information that could be used to resolve a case of repudiation for a registered and authenticated device.

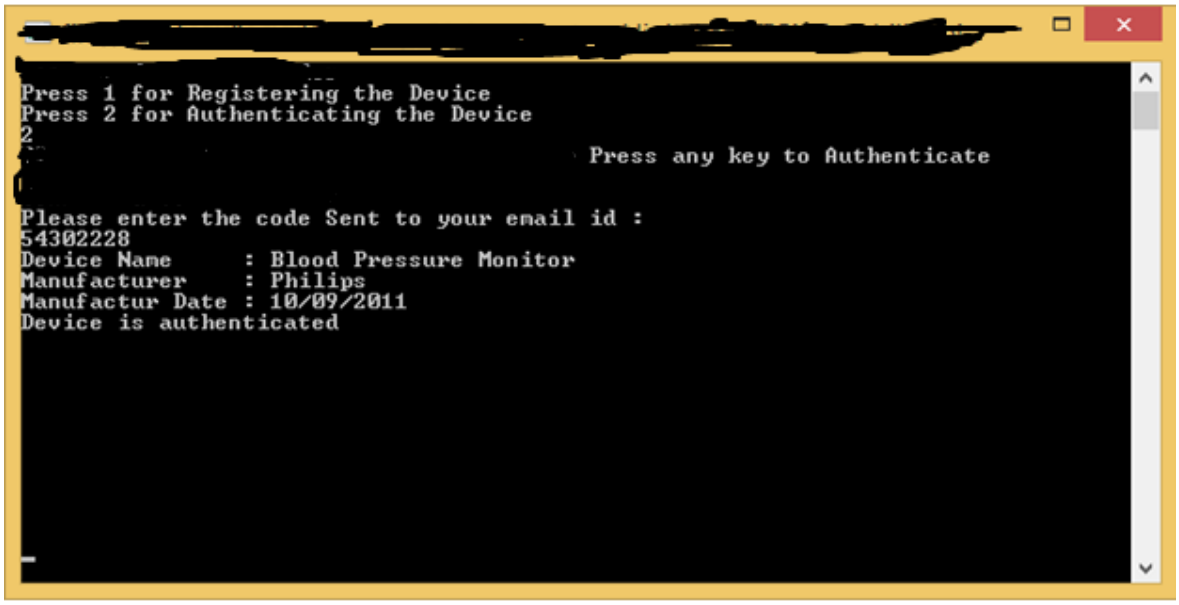

Figure II device authentication

4.2 Users Mailbox

The OTP is randomly generated and can only be used once during authentication.

In Figure III the user logs 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.

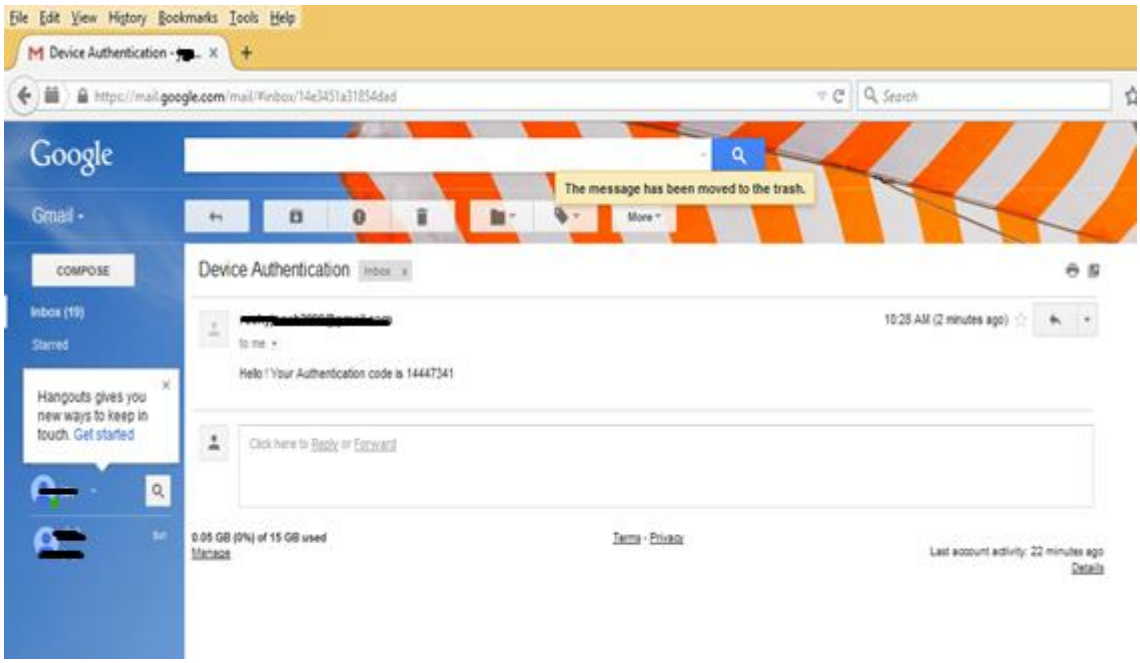

Figure III OTP sent to the mailbox of the patient

4.3 Patient Identification

Lack of a proper identification technique in PHD monitoring devices can lead to verification problems. If a patient cannot be properly verified they may not receive correct care, or worse may receive incorrect care.

This study recognises 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 Personal Health Devices (PHD).

NFC technology is proposed as a solution to the problem of identification of a patient using a PHD device. 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

Near field communication (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]:

1. 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.

2. 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 (TFL) network and in making payments at the grocery stores. This study identified that NFC technology will elicit different reactions, with most of them positive due to ease of use and very few negatives for those who are not familiar with the technology.

3. Cost

Cost plays a vital role in implementation of any technology. NFC technology is affordable and secure; an NFC card cost less than 40p and can be re-used multiple times by different users, which makes them economically viable.

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 with 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 is very sensitive and hence must be protected from tampering and unauthorised access. Furthermore, capabilities allow us to run a role-based mechanism so restrictions can be based on the role of different people within the healthcare 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 their roles. Figure IV present the new format that will be used to present capabilities. More details on this capability format is found in [15].

Figure IV. The new capability format.

The 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, applications, etc.
The Property Field: This field is used to define the properties of the object
The Object Id: This field is used to uniquely identify the object.
The Random Bit Field: This field helps to uniquely identify the object.
The Hash Field: The Hash field is used to prevent the casual tampering of capabilities.

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

5. CONCLUSION

The aim of this study was to determine the level of perception and knowledge of security among healthcare professionals. The outcome of this study indicates that the perception of healthcare professionals towards the importance of security is very low and their knowledge about security issues is poor. Such poor awareness of security amongst the users poses significant danger for the integrity of healthcare systems. This is especially important when adopting new technologies before all the threats are recognised 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 healthcare professionals are made aware of the security issues.

This study further identified specific threats to the implementation of telehealth. These include counterfeit remote patient monitoring devices and the identification and verification of the actual patient making observations. Digital signatures and OTP were proposed and investigated as a solution for device authentication and certify that the devices are genuine. Each device is bound to the patient that 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. WHO (2011) state that failure to correctly identify patients can result in wrong diagnosis, transfusion errors and testing errors. The USA 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 healthcare 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 8 participants agreeing to participate.

The approaches and results of this research can be used in the evaluation of security practices in the healthcare setting, and proposing best security practices in healthcare.

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].

Conflicts of interest statement

We wish to declare that there are no known conflicts of interest associated with this publication and there has been no financial support for this work that could have influenced its outcome.

REFERENCES

1. Huang, Ding-Long, Pei-Luen Patrick Rau, Gavriel Salvendy, Fei Gao, and Jia Zhou. Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies 69 (12) (12): (2011). 870-83.
2. Jeffrey Roman. The dangers of Patient Mismatches, Congress Urged to Study Data Mismatching Issue; 2012.
3. Ana Ferreira, Ricardo Correia, David Chadwicka , Luis Antunes, .Grounding Information Security in Healthcare; 2013.
4. Tesema, T., D. Medlin, and A. Abraham. Patient's perception of health information security: The case of selected public and private hospitals in Addis Ababa. Paper presented at Information Assurance and Security (IAS), Sixth International Conference; 2010.
5. Techtarget Medical Identity Theft. http://whatis.techtarget.com/definition/medical-identity-theft. Accesed March, 20, 2016
6. Shyam Natarajan, Christopher R. Wottawa and Erik P. Dutson Minimization of Patient Misidentification Through Proximity-based Medical Record Retrieval; (2009)
7. Vaibhav Garg, M.S. and Jefferey Brewer, M.S. Telemedicine Security: A Systemic Review. Journal of Diabetes Science and Technology; 2011.
8. Continua Health Alliance. Recommendations for Proper User Identification in Continua Version 1—PAN and xHR Interfaces. Retrieved July 8, 2016, Accessed from https://cw.continuaalliance.org/document/dl/download/3734; 2008.
9. Ondiege and Clarke (2014). Healthcare Professionals perception on Information Security: IADIS International conference Internet Technologies and society; 2014.
10. GS1, Healthcare White Paper on UDI implementation. Global standards pave the way for Unique Device Identification (UDI); 2011.
11. Petković, M. Remote Patient Monitoring: Information Reliability Challenges. Architecture, 295–301; 2009.
12. Defuse Encrypting One Time passwords. Available from: https://defuse.ca/eotp.htm. Accessed August 29,2015.
13. Martiri, Et al, Monotone digital signatures: an application in software copy protection. *Procedia Technology*, 1, (2012) pp.275–279.

14. Ondiege, Clarke & Mapp. Exploring security of Remote Patient Monitoring Devices using NFC technology for identification of the frail elderly; 8th International Conference of e-Health, IADIS;2016.
15. Mapp et al. Exploring a New Security Framework for Cloud Storage Using Capabilities. 1st International Workshop on Cyber Security and Cloud Computing, Oxford UK; 2014.
16. Amin, R. & Biswas, G.P... An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS. Journal of Medical Systems; 2015. 39(8), p.79.
17. 15 Mir, O., van der Weide, T. & Lee, C.-C., A Secure User Anonymity and Authentication Scheme Using AVISPA for Telecare Medical Information Systems. Journal of Medical Systems, 39(9), 2015 p.89.
18. WHO Impact, E., Patient identification policy., (2011),pp.1–26.
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 Lawfullness of the processing of personal Data